

Uniwersytet Szczeciński w Szczecinie  
Wydział Prawa i Administracji

**Artur Kolesiński**

# **Zastosowanie Internetu w prawie**

Praca magisterska napisana pod kierunkiem naukowym  
Dra hab. prof. US Andrzeja Balabana  
Katedra Prawa Konstytucyjnego i Integracji Europejskiej

Szczecin 20. maja 2001 roku.

Spis treści:

Wykaz skrótów s.6

## **Rozdział I.**

**Zagadnienia wstępne** s.7

## **Rozdział II.**

**Wpływ Internetu na prawo międzynarodowe oraz prawo Unii Europejskiej**

1. *Prawo międzynarodowe* s.11
  - *Organizacja narodów Zjednoczonych* s.11
  - *OECD i G 8* s.13
  - *Prawa autorskie* s.15
2. *Internet w Unii Europejskiej* s.16
  - *Spółeczeństwo informacyjne* s.17
  - *E- commerce* s.20
  - *Prawa autorskie* s.24
  - *Podpis elektroniczny* s.27

## **Rozdział III.**

**Zastosowanie Internetu w polskim prawie publicznym**

1. *Prawo Konstytucyjne* s.30
  - *Podstawowe prawa i wolności obywatelskie* s.30
  - *E-demokracja* s.32
2. *Prawo Karne materialne* s.33
  - *Zagadnienia ogólne i rodzaje przestępstw* s.34
  - *Pornografia w Internecie* s.36
  - *Hacking* s.39
  - *Kradzież programu komputerowego i Oszustwa komputerowe* s.42
  - *Inne przestępstwa* s.44
3. *Prawo Karne procesowe*
  - *Zagadnienia wstępne* s.46
  - *Czynności procesowe* s.47
  - *Dowody* s.48
  - *Podstęp telekomunikacyjny i elektroniczny* s.49

4.	<i>Prawo Prasowe</i>	
-	<i>Internet a prasa</i>	s.51
-	<i>Reklama w sieci</i>	s.52
-	<i>Prasa w Internecie i jej cenzura</i>	s.53
5.	<i>Prawo Finansowe</i>	s.55
-	<i>Prawo podatkowe</i>	s.56
-	<i>Prawo bankowe</i>	s.58
-	<i>Pozostałe działy prawa finansowego</i>	s.59

## **Rozdział IV.**

### **Zastosowanie Internetu w polskim prawie prywatnym**

1.	<i>Prawo pracy</i>	
-	<i>Przepisy kodeksu pracy a Internet</i>	s.62
-	<i>Telepraca</i>	s.63
2.	<i>Prawo cywilne materialne</i>	
-	<i>Oświadczenie woli</i>	s.67
-	<i>Zawieranie umów przez Internet i ich rodzaje</i>	s.69
-	<i>Forma pisemna</i>	s.71
-	<i>Podpis elektroniczny</i>	s.72
-	<i>Ochrona konsumentów</i>	s.75
-	<i>Dobra osobiste w Internecie</i>	s.76
3.	<i>Postępowanie cywilne</i>	s.76
-	<i>Pisma procesowe</i>	s.77
-	<i>Doręczenia</i>	s.77
-	<i>Dowody</i>	s.78
4.	<i>Prawo autorskie</i>	
-	<i>Przedmiot i podmiot prawa autorskiego</i>	s.80
-	<i>Eksploatacja i wprowadzenie utworu do sieci</i>	s.83
-	<i>Dozwolony użytek</i>	s.88
■	<i>Dozwolony użytek publiczny</i>	s.89
■	<i>Użytek osobisty</i>	s.90
-	<i>Umowy, tworzenie i eksploatacja produktów multimedialnych</i>	s.90

## **Rozdział V.**

### **Adresy internetowe, bazy danych i ich ochrona**

1.	<i>Domeny internetowe</i>	
-	<i>Uwagi wstępne oraz znaki towarowe</i>	s.93
-	<i>Nieuczciwa konkurencja</i>	s.97
2.	<i>Ochrona baz danych</i>	

-	<i>Bazy danych i ich ochrona w różnych uregulowaniach</i>	s.100
-	<i>Ochrona baz danych w Unii Europejskiej</i>	s.103
	<b>Zakończenie</b>	s.106
	<b>Wykaz aktów prawnych</b>	
1.	<i>Dokumenty polskie</i>	s.108
2.	<i>Dokumenty zagraniczne</i>	
-	<i>Akty prawne i inne dokumenty Unii Europejskiej</i>	s.108
-	<i>Akty prawne innych państw i organizacji</i>	s.109
3.	<i>Orzecznictwo</i>	s.109
	<b>Bibliografia</b>	
3.	<i>Wydawnictwa zwarte</i>	s.110
4.	<i>Czasopisma</i>	s.111
5.	<i>Inne</i>	s.112
6.	<i>Spis tabel</i>	s.113

## Wykaz skrótów:

- 1.BBS - Bulletin Board System
- 2.DNS - Domain Name System
- 3.EDI - Electronic Data Interchange
- 4.Dz.U. - Dziennik Ustaw
- 5.ICANN - Internet Corporation of Assigned Names and Numbers
- 6.IRC - Internet Relay Chat
- 7.k.c. - kodeks cywilny
- 8.k.k. - kodeks karny
- 9.k.p. - kodeks pracy
- 10.k.p.c. - kodeks postępowania cywilnego
11. k.p.k. - kodeks postępowania karnego
- 12.KPWiG - Komisja Papierów Wartościowych i Giełd
- 13.NASK- Naukowo Akademicka Sieć Komputerowa
- 14.OECD- Organization for Economic Co-operation and Development
- 15.ONZ - Organizacja Narodów Zjednoczonych
- 16.PIN - Personal Identification Number
- 17.PiP - Państwo i Prawo
- 18.PKB - Produkt Krajowy Brutto
- 19.pr.aut - ustawa z dnia 04 lutego 1994 r. o prawie autorskim i prawach pokrewnych
- 20.TAWF - Traktat WIPO w sprawie wykonań i fonogramów
- 21.TPA - Traktat WIPO o prawach autorskich
- 22.TRIPS - Agreement on Trade Related Aspects on Intellectual Property Rights including Trade in Counterfeit Goods
- 23.UE - Unia Europejska
- 24.UNCITRAL - United Nations Commission on International Trade Law
- 25.u.z.n.k. - ustawa z dnia 16.04.1993. o zwalczaniu nieuczciwej konkurencji
- 26.u.z.t. - ustawa z dnia 31.01.1985 o znakach towarowych
- 27.WIPO - World Intellectual Property Organization
- 28.WWW - World Wide Web
- 29.ZUS- Zakład Ubezpieczeń Społecznych

# Rozdział I.

## Zagadnienia wstępne

Internet stanowi przedmiot zainteresowania ze strony między innymi ekonomistów, polityków, socjologów i językoznawców. Grono nauk, na które wywiera on wpływ stale ulega zwiększeniu. Niniejsza praca dotyczy wpływu sieci komputerowej zwanej Internetem na prawo. Jak będziemy mieli okazję się przekonać owe oddziaływanie przebiega nie tylko w jedną stronę. Prawo także determinuje zmiany zachodzące w sieci.

Stosunkowo szybko dostrzeżono korzyści jakie może on przynieść, gdy zastosujemy go w wielu dziedzinach prawa. Postawiłem sobie jednak obok ukazania owych szans i korzyści za zadanie przedstawienie również problemów-zagrożeń, które sieć niesie ze sobą. Rola Internetu w prawie będzie się zwiększać. Dziś można powiedzieć, iż dostrzegamy owe przemiany lecz nie możemy w pełni ich docenić oraz przewidzieć ich skutków. Informacja w XXI wieku odgrywać będzie kluczową rolę. Internet to wręcz uosobienie informacji- szybkiej, skutecznej i obiektywnej.

Praca ta stara się choć w niewielkim stopniu przedstawić reakcję legislacji na te zdarzenia. Jak z każdą nowością tak i w przypadku Internetu należy „przetrzeć drogę”, „utorować szlak” – stworzyć uniwersalne rozwiązania, które będą na tyle elastyczne, aby ułatwiły rozwój tego medium nie zaś go zahamowały. Niejednokrotnie na łamach niniejszej pracy ukazuję toczące się spory wokół zasad tworzenia środowiska prawnego dla sieci. Różnorodność pojmowania wolności i prawa do informacji i słowa stanowi tu poważny problem. Możemy powiedzieć, iż właśnie te wartości są główną zasadą rządzącą Internetem. Dlatego też tak ważne jest prawo konstytucyjne w tej materii.

Jak jednak określić Internet? Jaka jest jego historia?<sup>1</sup> Trudno sobie wyobrazić i niewiele osób zdaje sobie z tego sprawę, iż korzenie Internetu sięgają zimnej wojny. Kamieniem węgielnym było stworzenie w 1957 roku w Departamencie Obrony Stanów Zjednoczonych projektu ARPA<sup>2</sup>. Szybko przekonano się, iż połączenie wielu komputerów (znajdujących się w wielu, różnych miejscach) stanowi swoistą rewolucję informatyczną. Nastąpiło to w roku 1969 i od tego czasu możemy datować początek Internetu. Zacytuję tu wypowiedź profesora Leonarda Kleinrock'a z uniwersytetu UCLA z tegoż roku: „Dziś sieci komputerowe są w fazie niemowlęctwa. Ale gdy dorosną [...], pewnie będziemy świadkami rozwoju branży sieciowej użyteczności publicznej, która tak jak dziś energetyka czy telekomunikacja będzie świadczyć usługi dla biur i domów w całym kraju”.

Od tego czasu datujemy gwałtowny rozwój sieci. W 1971 roku Ray Tomlinson opracował program do poczty elektronicznej (*e-mail*). Dziś jest ona najczęściej obok WWW stosowana przez użytkowników sieci (Forrester Research szacuje, iż w 2005 r. w Internecie będzie codziennie (!) krążyć 5 mld

---

<sup>1</sup>Na temat historii Internetu zob.: *A Brief History of the Internet*, na stronie WWW: <http://www.isoc.org/internet/history/brief.html>

<sup>2</sup> Advanced Research Projects Agency.

elektronicznych listów)<sup>3</sup>. Pierwsza domena internetowa (DNS- Domain Name System) pojawiła się w roku 1985- symbolics.com i od tego momentu ich ilość arytmetycznie zaczęła wzrastać.

Kolejnym wydarzeniem w powiększającej się sieci był wirus, który zainfekował 6600 komputerów (rok 1988). To był dopiero początek. Z czasem wraz z przyrostem liczby komputerów połączonych siecią (dziś są to już nie tylko komputery osobiste) skala wyrządzonych szkód i ilość zarażonych komputerów jest nieporównywalna.<sup>4</sup> Prawdziwą rewolucją było stworzenie technologii WWW- World Wide Web (która jest dziś niemal synonimem Internetu). Wymyślona w 1989 r. przez Tim'a Berners Lee zaczęła działać na dobre w roku 1991 momentalnie przynosząc ze sobą nową jakość w sieci. Rozwój właśnie WWW sprawił, iż stały się możliwe technicznie takie przedsięwzięcia jak handel elektroniczny czy chociażby e-prasa. Tak w olbrzymim skrócie wygląda historia tego nowego medium.

W niniejszej pracy często będziemy mogli spotkać się (już się spotkaliśmy) z synonimami słowa Internet. zamiennie stosuję tu takie określenia jak sieć oraz cyberprzestrzeń. Wyraźnie należy odróżnić od Internetu- Intranet, który jest siecią wewnętrzną- zamkniętą.

Duże trudności stwarza słownictwo techniczne związane z technologiami komputerowymi czy teraz także z samym Internetem. Często obok oryginalnych nazw posługuję się ich spolszczonymi wersjami (np. *e-mail* to list elektroniczny, poczta elektroniczna, *e-commerce* to e-handel, czy elektroniczna gospodarka, a z drugiej strony jest *hacking* nie mający polskiego odpowiednika). Jak widzimy na ostatnim przykładzie czasami nie można znaleźć polskiej wersji danego wyrazu. Wskazuje to dobitnie na charakter sieci, która stanowi wszak medium globalne (i najczęściej używanym językiem jest język angielski).

Praca niniejsza zawiera 5 rozdziałów łącznie z zagadnieniami wstępnymi. Wyodrębniłem zagadnienia prawa międzynarodowego oraz prawa Unii Europejskiej ze względu na istotność owych rozwiązań, które niewątpliwie mają wpływ na rozstrzygnięcia prawne dokonujące się w naszym kraju. Rozdział II zawiera mianowicie opracowane w skrócie dwa podrozdziały ukazujące związek Internetu z prawem międzynarodowym i prawem Wspólnot Europejskich. Poświęciłem dużo uwagi standardom przyjętym przez „15”, gdyż Polska w ramach spełniania kryteriów członkowskich wstępowania do Unii będzie musiała dostosować swe prawo właśnie pod kątem zastosowanych w Unii Europejskiej. Kolejne dwa rozdziały (Prawo publiczne i prawo prywatne) zasługują na szczególną uwagę. Na wstępie muszę wytłumaczyć dlaczego zastosowałem ów a nie inny podział polskiego prawa na owe dwa podzbiory. Sam podział wywodzi się od prawnika rzymskiego D. Ulpianusa (170-228), który w słynnym zbiorze *Corpus Iuris Civilis* stwierdził, że prawo publiczne służy ochronie bytu państwa rzymskiego, a prawo prywatne służy ochronie korzyści jednostki.<sup>5</sup>

Owe podzbiory wyodrębnia się na postawie różnych kryteriów:

---

<sup>3</sup> D. Ćwiklak, T. Bienias, konsultacja J. Donajski; *Encyklopedia Internet 1/ Narodziny sieci*, MAGAZYN nr 5 dodatek do Gazety Wyborczej nr 28, 2000/02/03.

<sup>4</sup> Przykładem jest tu wirus „I love you”.

<sup>5</sup> A.Redelbach, *Wstęp do prawoznawstwa*, Poznań 1996, s. 126.

- pozycji podmiotów związanych stosunkami prawnymi wyznaczonymi przez obowiązujące normy,
- rodzaju interesów chronionych przez normy prawne,
- rodzaju środków ochrony prawnej oraz sposobu korzystania z nich w celu zabezpieczenia realizacji obowiązujących norm<sup>6</sup>.

Dzięki tym kryteriom wydziela się trzy zasadnicze gałęzie prawa:

- prawo cywilne,
- prawo karne,
- i prawo administracyjne.

W części pracy szeroko poruszyłem problematykę Internetu w prawie karnym (Rozdział III) oraz prawa cywilnego (Rozdział IV). Zwraca uwagę brak w tym gronie prawa administracyjnego. Konieczne w tej kwestii jest kilka słów wyjaśnienia.

Nieobecność tej gałęzi prawa wcale nie dowodzi braku jego związku z Internetem. Wręcz przeciwnie. Są one rozległe i stale się zwiększają. Włączenie jednak prawa administracyjnego stanowiłoby nie lada wyzwanie lecz mogłoby urosnąć do rozmiarów całkiem oddzielnej pracy. Dodać także wypada, iż prawo administracyjne cechuje się bardzo specyficzną naturą, która jest odmienna od innych gałęzi prawa. Ramy pracy nie pozwoliły mi podobnie jak w przypadku prawa administracyjnego na dokładne przedstawienie problematyki ochrony dóbr osobistych w sieci oraz ochrony danych osobowych a także innych gałęzi prawa. Szczególnie te dwie ważne kwestie w przypadku Internetu nabierają znaczenia.

Wyodrębnienie i klasyfikacja różnych gałęzi w podzbiory jest często kontrowersyjne. Samo wyróżnienie gałęzi prawa ma charakter czysto praktyczny. Zaliczenie określonych przepisów do którejś z wyróżnionych gałęzi posiada tę istotną doniosłość praktyczną, że przepisy te będą interpretowane i stosowane zgodnie z przyjętymi w danej gałęzi zasadami prawa i w taki sposób, iżby zapewnić zgodność prakseologiczną i powiązania funkcjonalne z innymi normami tej gałęzi prawa<sup>7</sup>. Nie inaczej jest w mej pracy.

Sporne jest rozumienie prawa karnego i prawa pracy. W tych przypadkach zdecydowałem się je umieścić w dwóch różnych podzbiorych i właśnie w takich z wymienionych wyżej względów. Rozdział ostatni poprzedzający zakończenie nawiązuje do problematyki czysto internetowej. Bazy danych zrewolucjonizowała sieć a adresy internetowe są właśnie jej produktem. Ta ważna kwestia wymagała wyodrębnienia i zaakcentowania odrębności oraz ich znaczenia. Znaczenia, które jest zasadnicze w przypadku sieci komputerowych. Samo zakończenie stanowi próbę podsumowania rozważań zawartych w pracy oraz wskazania wniosków wpływających z przedstawionej problematyki. Całość zamyka spis literatury, która była mi pomocna w opracowaniu niniejszej pracy. Podkreślę jednak zasadniczy wpływ na niniejszą pracę książki Janusza Barty oraz Ryszarda Markiewicza *Internet a prawo*. Ta bodajże jedyna zbiorcza praca odnośnie

---

<sup>6</sup> S. Wronkowska, Z. Ziemiński, *Zarys teorii prawa*, Poznań 1997, s. 193, zob. także J. Nowacki, *Prawo publiczne – prawo prywatne*, Katowice 1992.

<sup>7</sup> S. Wronkowska, Z. Ziemiński, *Zarys teorii prawa*, op. cit., s. 194.

związków Internetu z prawem miała decydujące znaczenie przy wyborze przeze mnie tematu.

Zwracają uwagę podane przeze mnie źródła zaczerpnięte z Internetu. Trudno byłoby oprzeć się tylko i wyłącznie na „tradycyjnych” źródłach materiałów szczególnie pisząc o Internecie. Warto przed przystąpieniem do lektury oraz w jej trakcie uwzględnić pięć kluczowych zagadnień:

- a) Internet jako całość nie stanowi przedmiotu własności;
- b) Posiada on globalny charakter. Dane wprowadzone w jednym miejscu natychmiast stają się dostępne we wszystkich miejscach, do których dociera Internet;
- c) Rozwój Internetu jest zdumiewający. W styczniu 1998 r. zarejestrowanych było 107 mln użytkowników, a już w 2001 r. było ich ok. 414 mln<sup>8</sup>;
- d) Procesy zachodzące w sieci są aterytorialne, trudno je przypisać do określonego obszaru państwowego;
- e) Zachodzi splatanie się i przenikanie systemów komunikacji, telewizji kablowej, telefonów (telefonów komórkowych przede wszystkim), faksów, sieci komputerowych i mediów elektronicznych i audiowizualnych. Następuje splatanie się informatyki i telekomunikacji.<sup>9</sup>

Pamiętajmy o tych okolicznościach, gdy będziemy śledzić wpływ Internetu na prawo. Pamiętajmy w trakcie lektury także i o tym, iż praca zawiera przykładowe związki Internetu z niektórymi gałęziami prawa. Przy wyborze metody przybliżenia tych właśnie a nie innych i ich związków z Internetem kierowałem się doniosłością i charakterem wpływu na prawo. Praca nie stanowi zbiorczego i wyczerpującego przedstawienia tej problematyki. Można powiedzieć, iż jest niejako wstępem i ogniskuje naszą uwagę na najbardziej istotnych zagadnieniach. Praca niniejsza uwzględnia stan prawny na dzień 01. maja 2001 roku.

---

<sup>8</sup> Źródło: <http://www.netsizer.com/daily/TopCountry.html>.

<sup>9</sup> J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s.11.

## Rozdział II.

### Wpływ Internetu na prawo międzynarodowe oraz prawo Unii Europejskiej

#### 1. Prawo międzynarodowe

Globalne oddziaływanie Internetu stwarza duże problemy w różnych systemach prawnych. Pojawiają się one na przykład w prawie karnym, cywilnym, autorskim oraz międzynarodowym. Rola tego ostatniego polega przede wszystkim na usuwaniu przeszkód, zakazów, przejawów dyskryminacji w stosunkach między państwami oraz na ułatwianiu przepływu towarów, usług, kapitału i ludzi. Współpraca między narodami, przejawiająca się w funkcjonowaniu takich podmiotów jak Organizacja Narodów Zjednoczonych, OECD, G 8, Rada Europy<sup>10</sup>, Forum Ekonomiczne (DAVOS), czy Unia Europejska zmierza w kierunku wypracowania rozwiązań m.in. dotyczących Internetu. Bez owego współdziałania poszczególne państwa nie poradziłyby sobie z nowoczesnymi technologiami i ich wpływem na prawo.

Lecz jaki dokładnie wpływ na prawo międzynarodowe ma Internet? Spójrzmy na kilka wybranych zagadnień.

#### Organizacja Narodów Zjednoczonych

Główną rolę na arenie międzynarodowej odgrywa Organizacja Narodów Zjednoczonych. Także na jej łamach toczy się dyskusja o skutkach sieci komputerowych. Internet i ONZ łączy jedna podstawowa cecha- zakres działania- jest on globalny.

Sama Organizacja to tysiące urzędników, pracowników, tłumaczy i dyplomatów. Dzięki sieci Narody Zjednoczone mogą w pełni realizować swe podstawowe cele (artykuł 1 ustępy 1-3 Karty Narodów Zjednoczonych). Niezmierzone ilości papierowych dokumentów krążących po świecie, trudności i koszty w dotarciu do odległych zakątków globu na umówione spotkania czy konferencje, praca wielu tłumaczy- to wszystko sprawia, że koszty działania Organizacji są ogromne (pamiętajmy o problemach w zbieraniu składek członkowskich oraz niechęci ich płacenia).

Jak więc je obniżyć a jednocześnie usprawnić samo funkcjonowanie tej rzeszy ludzi? Rozwiązanie wydaje się być jedno - Internet i nowoczesne technologie telekomunikacyjne i informatyczne. Telekonferencje, elektroniczna wymiana dokumentów, poczta elektroniczna, komputerowe programy

---

<sup>10</sup> Rada Europy pracuje nad traktatem dotyczącym przestępstw elektronicznych (Cybercrime traty). Zob.R. Perera, *A step closer to becoming law*, "Infoworld" z 25.04.2001.

translacyjne- to wszystko może sprawić, o ile już nie sprawia, że Organizacja ulegnie przeobrażeniu. Możliwości, które daje sieć nie są jeszcze w pełni wykorzystywane, a w kierunku tym dużo należy zrobić. Spowoduje to również poprawę skuteczności w osiągnięciu celów oraz przede wszystkim ułatwi przepływ informacji. A to właśnie ona jest tutaj kluczowa.

Rok 2001 został proklamowany na mocy rezolucji Zgromadzenia Ogólnego z listopada 1998 r. (53/22) rokiem Dialogu między cywilizacjami<sup>11</sup>. Internet jak żadne medium może zapewnić wymianę poglądów na niespotykaną dotąd skalę. I choć dostęp do sieci nie jest jeszcze na świecie powszechny to liczba użytkowników gwałtownie rośnie<sup>12</sup>.

W styczniu 1997 roku na stronach WWW ONZ uruchomiono projekt cyfrowego szkolnego autobusu (*CyberSchoolBus*) stanowiący forum wymiany informacji i doświadczeń dla młodzieży szkolnej i studentów (program edukacyjny Departamentu Informacji Publicznej- Departament of Public Information – DPI). Co ciekawe już wtedy projekt ów postrzegany był jako program edukacyjny, z którego korzystać będą przyszli liderzy (wypowiedź Michael'a Eaton'a sekretarza generalnego National Model United Nations Conference (US)).<sup>13</sup>

Nie postrzegajmy Internetu tylko jako narzędzia usprawniającego pracę i obniżającego koszty. Organizacja Narodów Zjednoczonych (a właściwie jej wyspecjalizowane organy) zajmuje się nim także jako problemem prawnym. To właśnie jedna z głównych ról Narodów Zjednoczonych- wypracowywanie uniwersalnych rozwiązań.

Przejawem takiego działania jest modelowa ustawa UNCITRAL<sup>14</sup>, dotycząca zagadnień prawnych związanych z Elektronicznym Przekazem Danych (EDI) i pokrewnych środków komunikacyjnych. Zgromadzenie Ogólne Narodów Zjednoczonych w czerwcu 1996 roku na 29 sesji zatwierdziło ów projekt<sup>15</sup>. Samo to zagadnienie jest zbyt obszerne, aby się nim dziś tu zajmować. Przedstawię jednak jego ramowe założenia.

Pojęciem kluczowym w ustawie jest elektroniczna wiadomość (*data message*). Zgodnie z art. 2 (a) to informacja wytwarzana, przekazywana, przechowywana lub przesyłana przy pomocy środków elektronicznych, optycznych lub analogicznych, łącznie z EDI, pocztą elektroniczną, telegramem, teleksem i telefaksem. Zasadniczym punktem wzorcowej ustawy jest uznanie „prawnej doniosłości elektronicznego dokumentu i zrównanie go z innymi jego postaciami. Precyzyjnie podane są warunki pod jakimi uznać należy, iż spełniony został wymóg formy pisemnej. W ustawie zamieszczono także postanowienie dotyczące ustalania pochodzenia wiadomości elektronicznych, ich doręczania oraz wskazano no ich znaczenie w postępowaniu dowodowym.

Ustawa wzorcowa ma ogromne znaczenie. Po pierwsze dlatego, że była jednym z pierwszych rozwiązań dotyczących elektronicznej informacji, po drugie zaś była i pozostaje wskazówką dla ustawodawców krajowych jak powinni

---

<sup>11</sup> Press Briefing, 16.11.2000 r., Press Conference Launching web site on year of dialogue among civilizatinos.

<sup>12</sup> W 1991 r. Internet miał mniej niż 3 mln użytkowników na całym świecie, w 1999 r. było ich już 250 mln. ECO/WKP(2000)25 J.Copper, E-commerce: impact and policy challenges.

<sup>13</sup> Press Release 91/989 Model UN Discussion Area (MUNDA) Lunched on World Wide Web.

<sup>14</sup> United Nations Commissions on International Trade Law.

<sup>15</sup> Polski tekst ustawy wzorcowej możemy znaleźć w: W. Kocot, *Zawieranie umów sprzedaży według Konwencji Wiedeńskiej*, Warszawa 1998, s.269-277.

tworzyć ustawy o podpisach elektronicznych. Wyznacza drogę, którą poszczególne państwa mają zdążać dostosowując swe prawa do elektronicznego obrotu gospodarczego.<sup>16</sup>

Podobnych inicjatyw na łamach Organizacji należy oczekiwać więcej. To przecież ONZ ma inicjować prace w dziedzinie międzynarodowej współpracy rozwiązującej problemy, między innymi, Internetu. Widzimy więc, że sieć posiada ogromne znaczenie tak w usprawnianiu funkcjonowania jak i w prawnych zagadnieniach. Rola ONZ będzie w tej materii wzrastać, gdyż ona tak jak i Internet ma globalny zasięg działania i może sobie poradzić z wieloma wyzwaniami elektronicznej cywilizacji.

## OECD<sup>17</sup> i G 8

Cele działania Organizacji Współpracy Gospodarczej i Rozwoju, której Polska jest członkiem od 1996 roku, są podobne do celów gospodarczych ONZ. Nacisk położony został na koordynację polityki ekonomicznej, wspieranie rozwoju gospodarczego, wzrost zatrudnienia, poprawę poziomu życia obywateli i liberalizację handlu. Podstawowymi formami współdziałania jest wymiana informacji, dokonująca się poprzez konsultacje, doradztwo, konferencje, programy badawcze oraz opracowywanie strategii rozwoju.

Z uwagi na zakres owych zagadnień Internet nie mógł zostać pominięty w pracach organizacji. Dane statystyczne są jednoznaczne:

- po 1995 roku wzrost PKB w USA podwoił się, co najmniej 1/3 (jedną trzecią) ekonomicznego wzrostu stymuluje sieć, podobnie sytuacja wygląda w tworzeniu nowych miejsc pracy<sup>18</sup>,
- określany mianem *e-commerce* handel elektroniczny stanowi coraz bardziej znaczący element światowej ekonomii- wartość informatycznych technologii osiągnie w 2003 r. 3,2 trylionu dolarów (USD) i będzie to 5 procent Globalnego Produktu Brutto<sup>19</sup>.

Na łamach organizacji trwa dyskusja na temat wpływu Internetu na światową gospodarkę. Poza nią jednak pozostaje kwestia, iż wpływ ten będzie z roku na rok coraz większy. Rola OECD sprowadza się do wypracowywania wspólnych rozwiązań mających rozstrzygać problemy m.in. Internetu tak obecnie jak i w przyszłości. Problemem takim jest często brak odpowiedniego ustawodawstwa albo wręcz odwrotnie- jego nadmiar. Dla rządów najważniejsza jest jurysdykcja i kwestia jej uregulowania<sup>20</sup>.

Dlatego też tak ważna jest na tym polu międzynarodowa współpraca. OECD stanowi, odnoszące się do państw członkowskich, rezolucje i zalecenia jak reagować na dane zjawiska w sieci i e-gospodarce. Opracowuje główne założenia, które bazują na regulacji i samoregulacji problemu. W dyskusji uczestniczą nie

---

<sup>16</sup> Zob. J. Barta, R. Markiewicz, *Internet a prawo*, op.cit. s.96-99.

<sup>17</sup> Organization of Economic Co-operation and Development.

<sup>18</sup> Źródło: roczny raport Emerging Digital Economy – Departamentu Handlu USA z 1998 r. [www.ecommerce.gov/ederept.pdf](http://www.ecommerce.gov/ederept.pdf) -

<sup>19</sup> Źródło Forrester Reserch- amerykańskie towarzystwo badawcze.

<sup>20</sup> Patrz J. Dryden: *The work of the OECD on Electronic Commerce*. J.Dryden jest szefem Polityki Informacyjnej, Komputerów i Komunikacji w OECD w Paryżu.

tylko rządy państw członkowskich lecz także inne organizacje międzynarodowe i eksperckie<sup>21</sup>.

Przykładem rozwiązań na forum OECD jest kwestia opodatkowania sieci. Podczas ministerialnej konferencji (Ministerial Conference) w Ottawie w październiku 1998 roku opracowano pracę ramową dotyczącą warunków opodatkowania Internetu (Taxation Framework Conditions). Jest to baza, na której opierają się dalsze prace w tej materii. Kolejny krok naprzód uczyniono na konferencji w Paryżu, która odbyła się na przełomie stycznia i lutego tego roku (2001). Przewodniczący Komitetu do spraw Fiskalnych (Podatków) Gabriel Makhoul podkreślał potrzebę opodatkowania sieci.<sup>22</sup> Wypracowanie konsensusu jest niezbędne, gdyż konieczne stało się określenie miejsca opodatkowania, samego sposobu obliczania podatku oraz unikania podwójnego opodatkowania.

Handel ponad granicami sprawia, że dyskusja o jego skutkach implikuje przeniesienie debaty o problemach z nim związanych na szczebel międzynarodowy<sup>23</sup>. Ale cele, przed którymi stoi OECD to także: zapewnienie ochrony elektronicznych konsumentów, kryptografia, bezpieczeństwo w sieci, domeny internetowe oraz prywatność użytkowników. Wszystkie te zagadnienia wymagają szybkiego uregulowania, które będzie miało zasięg światowy. Dużym wyzwaniem jest budowa społeczeństwa informacyjnego<sup>24</sup>. Internet w OECD nie tylko ułatwia osiąganie wspólnych rozwiązań i usprawnia pracę ale stanowi również środek, który może zapewnić trwały i długofalowy rozwój tak członków tejże organizacji jak i pozostałych państw.

Organizacją, która ma ogromny wpływ na działanie OECD oraz na światową gospodarkę jest grupa G 8 (grupa państw G 7 powiększona o Rosję). Prezydenci oraz szefowie rządów grupy na corocznych szczytach dyskutują o najważniejszych wyzwaniach, które czekają na nas w XXI wieku.

Już w marcu 1994 r. na podobnym szczycie w Naples oraz na późniejszym spotkaniu ministerialnym w Brukseli w 1995 roku opracowano pilotowy projekt Globalnego Społeczeństwa Informacyjnego<sup>25</sup>. Postanowiono wtedy skupić się na takich dziedzinach jak:

- administracja publiczna,
- ochrona zdrowia,
- oraz środowiska,
- edukacja,
- i handel.

W każdej z nich przewidziano tworzenie specjalnych projektów (było ich 11), które będą stymulować rozwój informatycznych technologii w poszczególnych kwestiach.

---

<sup>21</sup> Law and Policy Forum (ILDF), oraz the Global Business Dialogue (GBDe).

<sup>22</sup> OECD Progresses Towards Achieving an International Consensus on the TAX Treatment of E-Commerce, Paryż 12.02.2001 r. – [www.oecd.org/media/relase/nw01-15a.htm](http://www.oecd.org/media/relase/nw01-15a.htm)

<sup>23</sup> S. Woodside w wypowiedzi dla „OECD Observer” z 06.02.2001 r.

<sup>24</sup> Na ów temat OECD zajęło stanowisko, patrz: Global Information Infrastructure- Global Information Society- GII-GIS Policy Recommendations for action OECD 1997 r.

<sup>25</sup> Towards A Global Information Society G 8 Global Information Society Pilot Projects Final Report. Dokument dostępny na stronie [www.gip.int/g8/mainreport.htm](http://www.gip.int/g8/mainreport.htm)

W przypadku edukacji programy te obejmują naukę przez uczniów, studentów, nauczycieli jak i obywateli języków obcych, wymianę doświadczeń i opinii. Ciekawym pomysłem jest tworzenie elektronicznych bibliotek, które zapewnią powszechny dostęp do posiadanych zbiorów. W 1995 roku myślano już o rządowych serwisach *on-line*, nastawionych na udzielanie pomocy obywatelom poprzez przekazywanie informacji: o pracach organów państwowych, aktach prawnych i prawach obywateli.

Od tamtego czasu świat i Internet bardzo się zmieniły. Wiele z tamtych koncepcji zostało zrealizowanych. Pozostałe wciąż są aktualne. Wymiana informacji, pomoc rządów w rozwoju sieci i społeczeństwa informacyjnego to tylko niektóre z nich. Organizacje międzynarodowe oraz grupa G 8 wyznaczają pewne kierunki postępowania. Droga do globalnego społeczeństwa informacyjnego wiedzie jednak nie tylko poprzez współpracę w ramach organizacji międzynarodowych. Duże znaczenie ma także rozwój stosunków bilateralnych oraz traktaty i konwencje dotyczące chociażby pośrednio Internetu i prawa.

## Prawa autorskie

Ogólnoświatowa sieć przyniosła ze sobą wiele problemów prawnych. Wypracowane rozwiązania w świetle nowych warunków musiały ulec zmianom. Internet wpłynął na porozumienia traktatowe akcentując swą obecność i doniosłość zachodzących zjawisk.

Konwencja Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów sporządzona w Wiedniu dnia 11.04.1980 roku nie przewidywała istnienia umów zawieranych za pośrednictwem sieci komputerowych. Dopiero ustawa modelowa UNCITRAL, o której już wspomniałem, uzupełniła przepisy konwencji o tą problematykę. Innym dobrym przykładem szybkiej reakcji dyplomatów na zmieniające się okoliczności są konwencje międzynarodowe z zakresu prawa autorskiego.

Porozumienia berneńskie i rzymskie nie przewidywały nowych technicznych możliwości eksploatacji utworów oraz artystycznych wykonań i fonogramów. Dynamika rozwoju Internetu sprawiła, iż niezbędne stało się uregulowanie praw autorskich w sieciach komputerowych. Brak owych działań mógł spowodować nawet gwałtowne zahamowanie wzrostu liczby użytkowników.

20. grudnia 1996 roku w Genewie uchwalono podczas konferencji dyplomatycznej odbywającej się w ramach WIPO (World Intellectual Property Organization) dwa nowe traktaty międzynarodowe. Konwencja WIPO dotycząca praw autorskich (WIPO Copyright Treaty) uzupełnia konwencję berneńską co do trzech podstawowych uprawnień majątkowych:

- Prawa do dystrybucji – art. 6. Prawem tym objęto wszystkie rodzaje utworów. Dopuszczono także wprowadzenie instytucji międzynarodowego wyczerpania prawa autorskiego.
- Prawa najmu – art. 7. Przedmiotem tego prawa są wyłącznie programy komputerowe, dzieła utrwalone w fonogramach oraz utwory kinematograficzne.<sup>26</sup>

---

<sup>26</sup> J.Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.197.

- Prawa do publicznego komunikowania – art. 8. Objęto nim utwory oraz takie formy udostępniania przy których użytkownicy posiadają dostęp do utworów z miejsca i w czasie przez siebie wybranym.

Z kolei druga konwencja WIPO w sprawie ochrony artystów wykonawców i producentów fonogramów (WIPO Performances and Phonogram Treaty) jest dostosowana do specyfiki korzystania z tych dóbr z pomocą sieci komputerowych<sup>27</sup>. Stanowi ona niejako „kopię” omówionej wcześniej autorskiej Konwencji WIPO.<sup>28</sup> Duże znaczenie w zakresie prawa autorskiego ma także Konwencja w sprawie handlowych aspektów praw własności intelektualnej (TRIPS)<sup>29</sup>, która stanowi załącznik do porozumienia w sprawie utworzenia Światowej Organizacji Handlu (WTO).

To tylko przykłady uregulowań traktatowych w dwóch dziedzinach prawa. Wiele problemów, które stwarza Internet nie zostało jeszcze rozwiązanych na arenie międzynarodowej (na przykład przestępstwa komputerowe mające swe skutki w wielu państwach czy jurysdykcja). W przedstawionych przeze mnie przykładach widać dobitnie, iż wpływ Internetu na prawo międzynarodowe jest znaczący. Jest to medium, które stale się rozwija, dokładne więc sprecyzowanie tego zjawiska nie jest jeszcze możliwe.

Trudno z dnia na dzień określić stopień jego wzrostu. Potrzeba perspektywy kilku lat, wnikliwej obserwacji i głębokiej analizy. Internet to dziś żywy organizm i przeprowadzanie na nim jakichkolwiek operacji (ingerencji z zewnątrz) może powodować skutki uboczne. Interwencja państw czy organizacji międzynarodowych w ten proces „dojrzewania” sieci jest jednak niezbędna, gdyż tylko ona może zagwarantować jego bezpieczny rozwój. Każde wtargnięcie w swobodę Internetu musi mieć poważne i uzasadnione podstawy. Takie działania mogą skutecznie podjąć przede wszystkim organizacje międzynarodowe poprzez merytoryczny dialog, uwzględnianie globalnego zasięgu sieci i wypracowywanie rozwiązań wspólnych, nie dla kilku państw lecz dla wszystkich podmiotów prawa międzynarodowego. To jest właśnie wyzwanie stojące przed wspólnotą międzynarodową w XXI wieku.

## 2. Internet w Unii Europejskiej

Do grona podmiotów decydujących o kształcie elektronicznego prawodawstwa należy Unia Europejska. Właśnie ona obok Stanów Zjednoczonych stanowi o charakterze zmian na tym gruncie. Unia posiada swą specyfikę. Tworzy ją wszak piętnaście suwerennych państw. Bez dialogu politycznego oraz współpracy nie można by było osiągnąć porozumienia Spójrzmy w jaki sposób Wspólnota próbuje sprostać wyzwaniu, które możemy nazwać „wpływem Internetu na prawo”.

---

<sup>27</sup> Ibidem, s.199.

<sup>28</sup> Ibidem.

<sup>29</sup> Agreement on Trade Related Aspects on Intellectual Property Rights including Trade in Counterfeit Goods.

## Spółeczeństwo informacyjne<sup>30</sup>

Jak możemy określić społeczeństwo informacyjne i dlaczego jest ono tak ważne? Na społeczeństwo informacyjne składają się między innymi:

- telepraca<sup>31</sup>,
- e-edukacja,
- telemedycyna,
- *e-commerce*,
- rząd *on line*,
- globalizacja gospodarki,
- nowa rola mediów.

Zagadnienie to wzbudza zainteresowanie nie tylko prawników lecz także socjologów, informatyków, ekonomistów i polityków.

Podstawową cechą takiego społeczeństwa jest aktywne i powszechne uczestnictwo obywateli w życiu społeczno - politycznym zarówno na szczeblu lokalnym jak i krajowym a czasami także globalnym<sup>32</sup>.

Rozpoczynając rozważania o społeczeństwie informacyjnym w Unii Europejskiej nie można pominąć pierwszego dokumentu, który zwracał uwagę Radzie Unii na ów właśnie problem. Mowa tu o tzw. raporcie Bangemanna<sup>33</sup>. Raport nazywał wydarzenia dokonujące się na naszych oczach rewolucją. Rewolucją opartą na informacji i nieskrępowanej prezentacji ludzkiej wiedzy w każdej formie - mówionej, pisanej i wizualnej bez względu na miejsce, czas i objętość. Podkreślono zmiany, które przeobrażają sposób w jaki pracujemy i żyjemy obok siebie. Raport obejmował takie dziedziny jak praca, nowy rynek usług, kryptografia, ochrona praw autorskich, technologia i wiele innych. Wskazywał również zagrożenia, które należy pokonać, aby udostępnić obywatelom w większym stopniu nowoczesne technologie. Dokument ten stanowił wyraźny sygnał, iż w społeczeństwie końca XX wieku następują szybkie i znaczące zmiany.<sup>34</sup>

Spójrzmy na chwilę jak kształtuje się społeczeństwo informacyjne w statystyce:

---

<sup>30</sup> Na temat społeczeństwa informacyjnego (informatycznego) zobacz: L.W. Zacher, *Świadomość społeczeństwa informatycznego (...)* [w:] *Spółeczeństwo informatyczne w perspektywie człowieka, technologii i gospodarki*, Warszawa 1999.

<sup>31</sup> Na temat telepracy piszę w rozdziale poświęconym prawu pracy.

<sup>32</sup> M. Maniecki, *Szanse i zagrożenia*, „Teleinfo” z 25.09.2000 r., nr 39/2000, s.33.

<sup>33</sup> Europa i społeczeństwo globalnej informacji, Zalecenia dla Rady Unii (Recommendations to the European Council „Europe and the global information society” z 16.05.1994 r. zauważyć należy, iż członkiem grupy (High- Level Group on the Information Society) był obecny przewodniczący komisji Europejskiej – Romano Prodi.

<sup>34</sup> We wrześniu 1997 r. opracowano nowy raport na potrzeby Unii Europejskiej zatytułowany „Nowy światowy porządek w komunikacji globalnej, potrzeba międzynarodowej karty”.

Tabela 1: Społeczeństwo informacyjne w 1999/2000 r. (w milionach).

	UE- „15”	USA	Japonia	Świat	Źródło
<b>Liczba komp.PC</b>	93	141	36	387	ITU*
<b>- na 100 mieszkańców</b>	25	52	29	6	
<b>Liczba hostów</b>	13.9	65.9	4.5	94.3	Netsizer*
<b>- na 100 mieszkańców</b>	3.7	23.9	3.9	1.6	
<b>Liczba użytkowników Internetu</b>	98	154	39	407	NUA*
<b>- na 100 mieszkańców</b>	26	56	31	7	
<b>Liczba telefonów komórkowych</b>	147	86	57	481	ITU*
<b>- na 100 mieszkańców</b>	39.7	31.7	45	8	

Źródło: Richard Deiss, Information Society Statistics, Strong growth of PC, Internet and mobile phone usage in the European Union, Statistics in focus, Industry, Trade and Services, Theme4- 4/2001

\*

- -ITU- International Telecommunication Union
- -Netsizer- [www.netsizer.com](http://www.netsizer.com)
- -NUA- [www.nua.ie](http://www.nua.ie)

Innym dokumentem był Plan działania Unii „droga Europy do społeczeństwa informacyjnego” – dokument Komisji z 19.07.1994 r. – COM (94)347 final.

Otwarta dyskusja o społeczeństwie informacyjnym doprowadziła we Wspólnotach do opracowania kolejnego dokumentu – eEurope. Inicjatywa ta ogłoszona została przez Romano Prodiego 08. grudnia 1999 r. Kolejne jej wersje opracowywano na szczytach w Lizbonie (23-24.03.2000 r.) i Feirze (19-20.06.2000 r.). Ostateczny kształt inicjatywy nazwanej eEurope 2002 (w tym właśnie roku muszą być osiągnięte zakreślone w niej cele) został ujęty w 3 grupy tematyczne rozwinięte w 11 punktów.<sup>35</sup> Przedstawię te najważniejsze z punktu widzenia społeczeństwa informacyjnego.

<sup>35</sup> W. Marciński, *E-rady dla Europy*, „Teleinfo” z 25.09.2000 r., nr 39/2000, s.33-34. Inicjatywa przewiduje 3 naczelnne cele. Są nimi:

1. przeniesienie każdego obywatela, domu, szkoły, przedsiębiorstwa i administracji w wiek cyfrowy,

a) E-edukacja. Edukacja jest bardzo ważnym czynnikiem determinującym wzrost ekonomiczny jak i społeczny oraz równość szans. Państwa Unii mają zapewnić:

- do końca 2001 roku wszystkim szkołom dostęp do Internetu,
- do końca 2002 r. nauczyciele mają być przeszkoleni w wykorzystywaniu sieci oraz multimediiów,
- uczniowie powinni mieć dostęp do szybkich łączy internetowych,
- do końca 2003 r. wszyscy powinni umieć posługiwać się komputerem oraz korzystać z Internetu.

Nie zapomniano o studentach oraz ośrodkach badawczych. W ramach eEurope postuluje się aby:

- do końca 2001 r. wszyscy studenci mogli korzystać z internetowych multimediiów z przynajmniej jednego wirtualnego uniwersytetu w każdym państwie członkowskim.

Zwrócono uwagę, iż już teraz kluczowym elementem akademickiego i zawodowego życia jest komunikacja poprzez pocztę elektroniczną. Jednak, aby zwiększyć przepływ informacji, a co za tym idzie także i poziom kształcenia, należy udostępnić akademickiej społeczności nowe źródła wiedzy (właśnie poprzez Internet).

b) Telemedycyna. Ochrona zdrowia dzięki sieci może zabrać całkowicie inny wymiar. Sprawa zabezpieczenia wysokiego jej poziomu dla każdego obywatela na przyszłość jest jednym z największych wyzwań stojących przed europejskimi rządami. W raporcie z 23-24 marca 2000 roku wspomina się, iż rządy „15” przeznaczają średnio 8% swoich PKB na ochronę zdrowia. Tylko 1 % z tych pieniędzy jest przeznaczany na informatyczną technologię. Ten niekorzystny trend starają się odwrócić twórcy eEurope. Postulują więc:

- aby do końca 2000 r. osiągnąć standaryzację informacji w dziedzinie medycyny,
- do końca 2003 r. powszechne było użytkowanie elektronicznych kart chipowych zapamiętujących informację medyczną
- oraz aby do końca 2004 r. wszyscy związani z telemedycyną byli połączeni do Internetu. Zapewnić ma to tak zapobieganie, diagnozowanie jak i samo leczenie pacjentów.

W dokumencie nie zapomniano także o niepełnosprawnych. Unia obejmuje ich szczególną ochroną (Deklaracja 22 traktatu Amsterdamskiego). Twórcy inicjatywy postulują, aby do końca 2001 r. strony WWW (publiczne) były dostosowane do potrzeb ludzi niepełnosprawnych (dotyczy to przede wszystkim osób niewidzących czy też niesłyszących).

c) Rząd *on line*. Już na wstępie w inicjatywie eEurope poświęcono elektronicznemu rządowi dużo miejsca. Zauważa się, iż wszyscy „elektroniczni obywatele” oraz przedsiębiorcy są zainteresowani lepszym i łatwiejszym dostępem do informacji sektora publicznego. Wskazuje się, iż wykorzystanie

---

2. stworzenie cyfrowo piśmiennej europy, wspieranej przez kulturę państw członkowskich gotową do przekazywania i rozwoju nowych idei,  
3. zapewnienie temu procesowi socjalnych podstaw, budowanie zaufania konsumentów i wzmocnienie społecznej spoiwości.

Internetu ułatwi realizację celów Traktatu Amsterdamskiego, zapewni dla obywateli pełną przejrzystość procesu podejmowania politycznych decyzji.

Wiele należy jeszcze zrobić, aby rządowe strony WWW były źródłem informacji o polityce rządów oraz prawodawstwie. Potencjalnymi korzyściami z zastosowania nowoczesnych technologii w rządzeniu będą między innymi:

- ograniczenie biurokracji i wydatków na nią
- uczynienie instytucji rządowych bliższymi obywatelom
- stworzenie lepszego europejskiego rynku informatycznego

Cele, które założono osiągnąć to przed wszystkim:

- łatwy dostęp *on-line* do informacji administracyjnych, kulturalnych, o ochronie środowiska oraz o rzeczywistych warunkach na drogach,
- umożliwienie składania zeznań podatkowych *on-line* oraz aplikacji o fundusze.

Inicjatywa eEurope to wyraz zaniepokojenia powiększającym się dystansem technologicznym pomiędzy Europą a Stanami Zjednoczonymi. To także drogowskaz do lepszego i bardziej otwartego społeczeństwa. Szanse, które stoją przed zjednoczoną Europą są olbrzymie i należy je wykorzystać. Internet może zapewnić nie tylko wzrost gospodarczy lecz, co jest głównym celem inicjatywy, większą integrację państw członkowskich.<sup>36</sup> Wskazuje się, iż jest to najwyższy czas, aby wykorzystać okazję, która często się nie zdarza („Such chances are rare”).

### *E-commerce*

Taką okazją dla Unii jest również handel elektroniczny (*e-commerce*). Podstawowym aktem w tej dziedzinie jest dyrektywa Parlamentu Europejskiego oraz Rady Europejskiej z 08.06.2000 r. w sprawie handlu elektronicznego<sup>37</sup>.

W preambule dyrektywy Parlament i Rada powołują się na Traktat Wspólnot Europejskich, w szczególności na artykuły 47 (2), 55 i 95, na propozycje Komisji<sup>38</sup> oraz opinię Komitetu Ekonomicznego i Społecznego<sup>39</sup>. Spośród wielu przyczyn uregulowania materii handlu elektronicznego warto zwrócić uwagę na następujące:

1. Unia Europejska dzięki *e-commerce* zamierza umocnić więzy między państwami a obywatelami wspólnot, zapewnić wzrost tak ekonomiczny jak i społeczny oraz zwiększyć wolny przepływ towarów i usług. Działania te mają na celu likwidację barier, które wciąż dzielą europejskie społeczeństwa (punkt 1 preambuły do dyrektywy o handlu elektronicznym).

2. Rozwój *e-commerce* jest olbrzymią okazją wzrostu zatrudnienia na obszarze Unii w szczególności w małych i średnich przedsiębiorstwach. Może on stymulować ekonomiczny wzrost oraz inwestycje w innowacyjne technologie przez europejskie firmy (2).

---

<sup>36</sup> “eEurope is intended to accelerate positiv change in the Union. It aims at ensuring this change towards the Information Society is cohesiv, not divisiv. Intergating not fragmenting.”

<sup>37</sup> Directiv 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (Directiv on electronic commerce) Official Journal L 178.17/07/2000 p.0001-0016.

<sup>38</sup> OJ C 30, 5.2.1999, p. 4.

<sup>39</sup> OJ C 169, 16.6.1999, p. 36.

3. Dyrektywa ma także na celu zapewnić pewność i zaufanie konsumentom (punkt 7).

4. W zakres przepisów dyrektywy nie wchodzi materia opodatkowania, w szczególności podatku VAT (12 i 13).

5. Państwa członkowskie są zobligowane do usunięcia przeszkód przy stosowaniu elektronicznych umów (38 i 39).

6. Ważnym zapisem jest punkt 59, w którym zauważa się globalną naturę elektronicznej komunikacji, koordynacji z międzynarodowymi uregulowaniami. Należy unikać rozbijania (fragmentation) jednolitego Rynku. Dyrektywa ma zapewnić wspólną i silną (common and strong) pozycję Unii na forach międzynarodowych w przedmiocie *e-commerce*.

7. Przepisy powinny być proste i zrozumiałe, zwarte i przewidywalne (predictable) oraz stosowane do zasad na poziomie międzynarodowym (60).

8. Współpraca z państwami trzecimi powinna być silniejsza w tym obszarze w szczególności z państwami kandydackimi, rozwijającymi się i innymi partnerami handlowymi.

9. Elektroniczna komunikacja oferuje państwom członkowskim wsłania środki prowadzenia usług publicznych w kulturze, edukacji i nauce języków (64)

Po ogólnym omówieniu założeń warto przyjrzeć się samym przepisom dyrektywy. W artykule 1 zostały określone cele oraz zakres (objectiv and scope). Podstawowym celem jest zapewnienie lepszego funkcjonowania Jednolitego Rynku przez zapewnienie wolnego przepływu usług w społeczeństwie informacyjnym w państwach członkowskich. Dyrektywa uzupełnia prawo Wspólnot Europejskich w tej materii bez szkody dla poziomu ochrony w szczególności w ochronie zdrowia i konsumentów. Przepisy nie regulują polityki podatkowej, prawa antymonopolowego oraz innych obszarów (artykuł 1. 4 i 5).

Zwracają uwagę sformułowane w artykule 2 definicje (information society services, service provider, consumer, recipient of the service, commercial communications, regulated profession).

Ważną kwestią jest uzupełnienie przepisów o Jednolitym Rynku (art. 3). Państwa członkowskie mogą nie przestrzegać wolności do prowadzenia informatycznych usług z innego państwa członkowskiego tylko z określonych powodów. Takimi przesłankami mogą być między innymi: ochrona zdrowia, polityka publiczna w szczególności prewencja, śledztwo, wykrywanie i karanie przestępstw kryminalnych, bezpieczeństwo publiczne i ochrona konsumentów.

W rozdziale II zawarto generalne zasady. Warto zwrócić uwagę na przepisy dotyczące handlowej komunikacji (art. 6, 7 i 8), zawierania umów elektronicznych (art.9), odpowiedzialności pośrednich dostawców usług (art. 12-15). Ciekawy jest w szczególności art. 13 regulujący kwestię *cachingu* oraz art. 14 - *hosting* Artykuł 15 stwierdza, iż państwa członkowskie nie mogą nakładać obowiązków na dostawców, gdy dostarczają usług w rozumieniu art.12-14, monitorowania informacji, które oni transmitują lub sprzedają, ani generalnego obowiązku aktywnego śledzenia wydarzeń czy okoliczności wskazujących na nielegalne działanie (art.15.1).

Rozdział III poświęcono przyjęciu przepisów dyrektywy. IV natomiast dotyczy postanowień końcowych . Zawarto w nim zalecenie dla państw „15”

wdrożenia w życie regulacji przewidzianych w dyrektywie do 17.01.2002 roku<sup>40</sup>. Tak krótki okres czasu na dostosowanie prawa dla krajów członkowskich jest wyrazem pośpiechu, nadrabiania zaległości, które Europa ma przede wszystkim w stosunku do Stanów Zjednoczonych<sup>41</sup>.

Z dyrektywą o handlu elektronicznym bezpośrednio związana jest informacja Komisji Europejskiej dla Parlamentu i Rady w sprawie e-handlu i usług finansowych (Communication from the commission to the Council and the European Parliament, E-commerce and financial services).<sup>42</sup> Uchwalenie dyrektywy o e-commerce stworzyło konieczność zapewnienia spójności legislacji dotyczącej usług finansowych oraz e-handlu (gospodarki jak czasami tłumaczy się *e-commerce*). Komisja wskazuje, iż postanowienia opracowane na szczycie w Lizbonie przez Radę Europejską przewidują termin ostateczny (rok 2005) do ustanowienia zintegrowanego (Jednolitego) Rynku w usługach finansowych. Jest to osią planu Wspólnoty w polityce pracy i planowanym wzroście ekonomicznym. Informacja Komisji określa 3 obszary, w których nowa polityka ma być rozwijana i ochraniana:

- program skupienia zasad-przepisów (rules) ochrony kontraktowej (umownej) i niekontraktowej,
- celowe kroki zmierzające do poprawy zaufania konsumentów w wynagrodzeniach między granicami i internetowych należnościach (internet payments),
- zapewnienie nadzorowania współpracy.

Komisja we wstępie zauważa, iż nowa technologia już ma ogromny wpływ na przemysł usług finansowych. Rewolucjonizuje operacje na całym rynku, transformuje (zmienia) zasady świadczenia usług między państwami (cross-border services) i działa jak katalizator w tworzeniu nowych usług finansowych i nowych modeli biznesu. Często stanowi przyczynę fuzji w telekomunikacji, firmach informatycznych technologii, sprzedaży detalicznej czy w usługach finansowych.

Aby osiągnąć cele, określone przez Radę Europejską w Lizbonie Komisja bada (explores) trzy nowe obszary w komunikacji, szczególnie w kontekście implementacji dyrektywy o handlu elektronicznym:

I. Należy zaadoptować aktualne regulacje i przepisy, szczególnie dokonać ich skupienia w ochronie konsumentów i inwestycji dla obu rodzajów zobowiązań (kontraktowych i niekontraktowych).

II. Należy rozwinąć sposoby zapewnienia bezpieczeństwa systemów zapłaty i pozasądowych odszkodowań na bazie międzypaństwowej.

III. Osiągnąć zwiększenie nadzoru współpracy co może implikować nowe wyzwania międzynarodowe.

W punkcie trzecim dokumentu (zapewnienie spójności w strukturze legislacyjnej dla usług finansowych) Komisja wskazuje na sposoby osiągnięcia

---

<sup>40</sup> Dyrektywa weszła w życie w dniu publikacji w oficjalnym dzienniku – 17.07.2000 r.

<sup>41</sup> Zob. K. Niklewicz, *Najpierw prawo, potem boom*, „Gazeta Wyborcza” z 10.04.2000 r.

Stany Zjednoczone kwestię e-commerce uregulowały w : *Electronic Signatures in Global and National Commerce Act* z 24.01.2000 r. oraz w: *A Framework for Global Electronic Commerce* z 01.07.1997 r.

<sup>42</sup> Zob. J. Pawlicki, *Jak dogonić Amerykę*, „Gazeta Wyborcza” z 24.03.2000 r.

wysokiego poziomu zharmonizowanej ochrony wewnątrz Wspólnot w takich dziedzinach jak:

- handlowa komunikacja (3. Strand I (i)),
- marketing (ii),
- bankowość (kredyty hipoteczne, konsumenckie) (Strand II (i)),
- usługi inwestycyjne (ii),
- ubezpieczenia (iii),
- oraz niezharmonizowanych obszarach (iv).

W punkcie 4 (policy area II- budowa konsumenckiego zaufania w rekompensatach i internetowych systemach płatności) zawarto przykładowe dalsze skutki (wiele nie uregulowanych) planowane do zabezpieczenia zaufania konsumentów w postanowieniach usług finansowych *on line*. Podzielono je na 2 grupy. Pierwszą stanowi potrzeba szybkiego i efektywnego dostępu do odszkodowań w przypadkowych zdarzeniach. Drugą natomiast znaczenie liczby specyficznych spraw w użytkowaniu nowych technologii włączając w to bezpieczeństwo i odpowiedzialność z tytułu internetowych systemów płatności. W punkcie 5 (policy area III- zapewnienie nadzoru współpracy) wskazuje się na zagrożenia, które muszą być uregulowane i brane pod uwagę także w gospodarce elektronicznej (np. pranie brudnych pieniędzy, procedury zawiadomień).

W punkcie 6 (next steps) Komisja wskazuje jeszcze raz na potrzebę podjęcia szybkich kroków zmierzających do harmonizacji przepisów usług finansowych *on line*.

Ważnym zagadnieniem, które cały czas podkreślają organy Unii Europejskiej są prawa konsumentów, w sieci szczególnie narażonych na niekorzystne praktyki za strony usługodawców czy sprzedawców. Unia wypracowała tym zakresie bardzo szczegółowe rozwiązania. Trudno byłoby je wszystkie wymienić i opisać. Zauważyć jednak należy, iż najważniejszymi dokumentami w tej materii są dyrektywy:

- Dyrektywa 85/577 EWG z 20.12.1985 r. w sprawie ochrony konsumentów przy umowach zawieranych poza miejscem prowadzenia handlu,
- Dyrektywa 97/7 EC parlamentu Europejskiego i Rady z 20.05.1997 r. w sprawie ochrony konsumentów w odniesieniu do umów zawieranych na odległość.

W powiązaniu zaś z systemami płatności:

- Dyrektywa 2000/28/EC i 2000/46/EC w sprawie e-pieniędzy (mogą być one użyte tylko pod kontrolą odpowiednich instytucji pod prawnymi i finansowymi warunkami i po zapewnieniu technicznego bezpieczeństwa),
- Rekomendacja 97/489/EC dotycząca transakcji pokrywanych przez elektroniczne systemy płatności.

Ważnym dokumentem jest również Action Plan on promoting safer use of the Internet (decyzja nr 276/1999 EC, Europejskiego Parlamentu i Rady z 25.01.1999 r.). To tylko najbardziej doniosłe akty prawne w materii ochrony konsumenta. Widzimy więc, iż zaraz za deklaracjami ochrony konsumenta idą konkretne działania. Bezpieczeństwo transakcji *on line* oraz ochrona konsumenta i inwestorów są jednymi z najważniejszych celów Unii Europejskiej w kwestii Internetu.

Handel elektroniczny jest przedmiotem innych dokumentów unijnych. W inicjatywie eEurope – An Information Society For All mowa jest (w punkcie 3) o przyspieszeniu e-handlu. Przyjęto założenia, na których jak mogliśmy zauważyć opierają się dalsze działania Unii. Do końca 2000 r. miano osiągnąć:

- Rada i Parlament miały dołożyć wszelkiego wysiłku, aby zapewnić, że pozostałe wiążące się z e-handlem dyrektywy będą przyjęte,
- Komisja miała wspierać stworzenie domeny (Top Level Domain) .eu,
- Komisja miała zaproponować zmiany w Unii procedur dostaw publicznych tak aby uznawały elektroniczne środki we wszystkich publicznych procedurach i transakcjach.

W punkcie 6 inicjatywy zwrócono uwagę na znaczenie małych i średnich przedsiębiorstw (SME- small and medium enterprises).

Wspomnieć należy także o tzw. Green Papers<sup>43</sup>. Dwa z nich koniecznie trzeba wymienić:

- Green Paper on Commerce COM (96)530, November 1996,
- Commercial Communications in the Internal Market- Green Paper from the Commission COM (96)192, April 1996.

## Prawa autorskie

Wpływ Internetu na prawo nie mógł zostać nie zauważony w takiej dziedzinie jak prawo autorskie. Przesyłanie cyfrowych utworów (czy ich wersji) w sieciach komputerowych powoduje, że w tym samym czasie miliony użytkowników mają możliwość zapoznania się z nimi- bezpośrednio ich percepcji

W prawodawstwie Unii Europejskiej kwestia praw autorskich i praw pokrewnych w środowisku elektronicznym jest przedmiotem wzmoczonych ostatnio prac. Już w 1995 roku w Green Papers on Copyright and Related Rights in the Information Society Komisja Europejska zwróciła uwagę, iż podstawowe znaczenie dla rozwoju rynku wspólnotowego ma uregulowanie tej problematyki.<sup>44</sup> Ostatecznie w 2000 r. Komisja przedstawiła nową wersję projektu, która charakteryzuje się rozszerzeniem katalogu sytuacji umożliwiających korzystanie z utworów i przedmiotowych praw pokrewnych w ramach dozwolonego użytku.<sup>45</sup>

Projekt nawiązuje do dwóch traktatów Międzynarodowej Organizacji Własności Intelktualnej (WIPO) o prawie autorskim i o artystycznym wykonaniu i fonogramach<sup>46</sup>. W preambule projektu dyrektywy zawarto postulat usunięcia stanu niepewności w zakresie charakteru i poziomu ochrony działań – rozpowszechniania i udostępniania za pośrednictwem sieci komputerowych. Jest on oceniany negatywnie i dlatego też konieczne jest jego usunięcie. Tak z preambuły, jak i z art. 1 projektu dyrektywy wynika, iż poza nielicznymi

---

<sup>43</sup> Są to komunikaty publikowane przez Komisję w specyficznych dziedzinach, początkowo są one adresowane do zainteresowanych partii, organizacji, indywidualnych odbiorców, którzy są zapraszani do uczestnictwa w procesie konsultacji i dyskusji na ten temat. Prowadzą one w wielu przypadkach do dalszej (późniejszej) legislacji.

<sup>44</sup> Dokładna historia prac nad projektem dyrektywy znajduje się w: A. Matlak, *Prawo autorskie i prawa pokrewne w społeczeństwie informacyjnym z punktu widzenia projektu nowej dyrektywy Unii Europejskiej*, „Radca Prawny” 01/2001 oraz w: J.Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 201.

<sup>45</sup> A. Matlak, *Prawo autorskie i prawa pokrewne...*, op. cit., s. 12.

<sup>46</sup> Zob. na ten temat w podrozdziale dotyczącym prawa międzynarodowego.

przypadkami nie narusza ona obowiązujących w ramach Unii Europejskiej regulacji w przedmiocie praw autorskich i praw pokrewnych.<sup>47</sup> Potwierdzono w ten sposób zasadę, która obowiązuje we Wspólnotach tzw. *acquis communautaire* – dorobku prawnego wspólnoty.

Przepis art. 2 projektu dyrektywy dotyczy przyznania przez państwa członkowskie prawa wyłącznego do zwielokrotniania na rzecz:

- autorów – w odniesieniu do ich utworów,
- artystów wykonawców- w odniesieniu do ich wykonań,
- producentów fonogramów- w odniesieniu do ich fonogramów,
- producentów pierwszych utrważeń filmów- w odniesieniu do oryginału i kopii ich filmów,
- organizacji nadawczych- w odniesieniu do utrważeń nadawanych przez nie programów, niezależnie od tego, czy są one przekazywane drogą przewodową, czy drogą radiową (włączając w to przekaz satelitarny).<sup>48</sup>

Prawo do reprodukcji obejmuje tak bezpośrednie jak i pośrednie tymczasowe oraz trwale zwielokrotnianie wszelkimi środkami w każdej postaci tak całości, jak i części przedstawionych wyżej przedmiotów ochrony. Owa szeroka definicja wyłącznego prawa zwielokrotniania miała na celu wskazanie, iż prawo to dotyczy także eksploatacji chronionych dóbr również w Internecie (w sieciach komputerowych).

Istotne jest objęcie prawem reprodukcji jej tymczasowej postaci<sup>49</sup>. Do wykonywania prawa do faktycznego korzystania z utworów i przedmiotowych praw pokrewnych w sieciach komputerowych wystarczy samo wprowadzenie chronionego utworu do sieci, w ten sposób, iż osoby z niego korzystające mogą „na żądanie” doprowadzić do jego przekazu. W celu podkreślenia wyłącznego charakteru prawa do publicznego udostępniania w art. 3 projektu wskazano na to, iż nie ulega ono wyczerpaniu przez żaden akt publicznego rozpowszechniania.<sup>50</sup>

W preambule projektu dyrektywy oraz w jej art. 5 zamieszczono wszystkie przypadki ograniczenia praw wyłącznych przyznanych uprawnionym podmiotom i autorom, powinny być one stosowane wyłącznie w szczególnych sytuacjach. Natomiast ich rozszerzająca interpretacja jest niedozwolona. Zaznaczono także, iż z chronionych dóbr w ramach dozwolonego użytku korzystać należy w poszanowaniu słusznym interesów podmiotów uprawnionych oraz nie można naruszać normalnej eksploatacji utworów i przedmiotów praw pokrewnych.

Postanowienie art. 5 (2) (b) projektu określa możliwość wykorzystania utworów i chronionych dóbr w ramach użytku prywatnego.<sup>51</sup>

---

<sup>47</sup> Mowa tu o regulacji dotyczącej m.in. ochrony programów komputerowych, ochrony baz danych, praw autorskich i praw pokrewnych w odniesieniu do przekazu satelitarnej retransmisji i kablowej. Por. A. Matlak, *Prawo autorskie i prawa pokrewne...*, op. cit., s. 14.

<sup>48</sup> Podział przytoczony za: A. Matlak, *Prawo autorskie i prawa pokrewne...*, op. cit., s. 14.

<sup>49</sup> A. Matlak, *Prawo autorskie i prawa pokrewne...*, op. cit., s. 15.

<sup>50</sup> Ibidem, s. 16.

<sup>51</sup> Państwa członkowskie mogą ustanowić ograniczenia owego wyłącznego prawa do reprodukcji określonego w art. 2 projektu pod warunkiem, że podmioty uprawnione otrzymają uczciwe wynagrodzenie, uwzględniające zastosowanie lub nie środków technicznych (mowa jest o nich w art. 6.) względem danego utworu lub przedmiotu praw pokrewnych. Takie sformułowanie wskazuje, iż uprawnionym przysługuje prawo do wynagrodzenia. Stanowi to odstępstwo od światowych standardów, które takiej możliwości nie przewidują. Jak

W art. 5 (3) wskazano na większy katalog wyjątków odnoszący się do prawa do publicznego udostępniania (publiczny dozwolony użytek). Mogą one dotyczyć m.in.:

- reprodukcji w prasie, publicznego udostępniania opublikowanych artykułów na temat bieżących zagadnień gospodarczych, politycznych czy religijnych (...),
- przytaczania cytatów dla potrzeb takich jak analiza krytyczna czy recenzja, pod warunkiem że odnoszą się one do utworu lub przedmiotu praw pokrewnych, który został już zgodnie z prawem publicznie udostępniony odbiorcom a tam gdzie jest to możliwe, wskazane zostało źródło, w tym nazwisko twórcy,
- korzystania z takich utworów, jak dzieła architektoniczne lub rzeźby, wykonanych z myślą o ich umieszczeniu na stałe w miejscach publicznych.<sup>52</sup>

Zgodnie z wcześniejszą uwagą pamiętajmy, iż do niektórych konkretnych przypadków dozwolonego użytku publicznego dołączony jest obowiązek zapłaty wynagrodzenia na rzecz uprawnionego podmiotu.

Rozwój technologii cyfrowej sprawił, iż pojawiły się dotąd nieznanne zabezpieczenia przed korzystaniem z utworów i przedmiotowych praw pokrewnych przez osoby nieuprawnione do tego. Istnieją środki techniczne pozwalające na wprowadzenie elektronicznych oznaczeń identyfikujących chronione dobra oraz stwierdzające kto i kiedy i w jakim zakresie je wykorzystywał.<sup>53</sup> Projekt dyrektywy tej problematyce poświęca dużo uwagi. Art. 6 przewiduje, iż państwa członkowskie będą zobowiązane do zapewnienia ochrony prawnej przed obchodzeniem wszelkich skutecznych środków technicznych mających chronić prawa autorskie i pokrewne oraz prawa *sui generis* w stosunku do baz danych, którego jednostka dokonuje świadomie lub posiada wystarczającą wiedzę by przewidzieć cel do którego dąży.

Projekt posuwa się jeszcze dalej. Mianowicie można wywnioskować z art. 6 (2), iż ochrona ma być wprowadzona także przed czynnościami „przygotowawczymi” zmierzającymi do usunięcia zabezpieczeń.<sup>54</sup> W art. 6 zawarto także definicję środków technicznych, przez które rozumie się – każdą technologię, urządzenie lub jego element (składnik, który w normalnych warunkach działania ma na celu zapobieganie lub ograniczanie naruszania praw autorskich i praw pokrewnych oraz prawa *sui generis* przysługującemu bazom danych).<sup>55</sup>

Projekt dyrektywy zezwala państwom członkowskim na złagodzenie skutków ochrony technicznych zabezpieczeń przede wszystkim w sytuacjach, gdy podmioty uprawnione w sposób nieuzasadniony uniemożliwiają dostęp do nich

---

zauważa A. Matlak rozwiązać ów problem można stosując tzw. system obowiązkowych opłat od czystych nośników. Zob. A. Matlak, *Prawo autorskie i prawa pokrewne...*, op. cit., s. 17-18.

<sup>52</sup> A. Matlak, *Prawo autorskie i prawa pokrewne...*, op. cit., s. 18-19.

<sup>53</sup> Ibidem, s.20.

Problematyka ta była przedmiotem obrad w trakcie konferencji dyplomatycznej w Genewie. Efektem tego są odpowiednie postanowienia art.11 i 12 TPA oraz art. 18 i 19 TAWF – (odpowiednio – Traktat o prawie autorskim oraz Traktat o artystycznych wykonaniach i fonogramach).

<sup>54</sup> Por. J. Barta, R. Markiewicz, *Prawo autorskie*, Warszawa 1998, s. 119., zob. także: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit.

<sup>55</sup> A. Matlak, *Prawo autorskie i prawa pokrewne...*, op. cit., s.21..

dla osób zainteresowanych (art.6 (4)). Art. 7 projektu dotyczy ochrony elektronicznych środków identyfikacji utworów i przedmiotowych praw pokrewnych, które umożliwiają zarządzanie tymi prawami. Na temat prawa autorskiego i Internetu oraz wokół projektu dyrektywy toczą się na łamach Unii dyskusje.

## Podpis elektroniczny

Ścisły związek ze społeczeństwem informacyjnym oraz z prawem autorskim ma kwestia podpisu elektronicznego. Można śmiało powiedzieć, że odgrywa on tutaj kluczową rolę.

Prace nad dyrektywą o podpisie elektronicznym trwały od 1997 roku<sup>56</sup>.

13. grudnia 1999 r. uchwalono dyrektywę Parlamentu Europejskiego i Rady o ramowych założeniach Wspólnot dotyczących podpisów elektronicznych<sup>57</sup>. Preambuła dyrektywy zakłada, iż elektroniczne podpisy będą stosowane w różnych okolicznościach i podaniach wynikających z dużego zasięgu nowych usług i produktów. Inny punkt (14) dotyczy zachowania równowagi między potrzebami konsumentów a biznesu. Ważnym punktem jest punkt 19, który przewiduje stosowanie podpisów elektronicznych w sektorze publicznym wewnątrz narodowych i unijnych struktur administracji i komunikację pomiędzy tymi podmiotami a obywatelami i ekonomicznymi operatorami. Podano nawet przykładowe dziedziny, w których takie kontakty będą nawiązywane:

- w podatkach,
- bezpieczeństwie publicznym,
- ochronie zdrowia,
- sądownictwie,
- zamówieniach publicznych<sup>58</sup>.

Punkt (20) zakłada zrównanie mocy prawnej kwalifikowanych podpisów elektronicznych z podpisami ręcznymi.<sup>59</sup>

W art. 1 określono cel zastosowania przepisów dyrektywy. Mają one ułatwić stosowanie podpisów elektronicznych i wnieść wkład w ich prawne uznawanie. Innym celem jest zapewnienie lepszego funkcjonowania Jednolitego Rynku.

Definicje zawarte w art. 2 (13) mają za zadanie rozwiązać wiele przyszłych problemów w pojmowaniu użytych sformułowań. Warto przytoczyć definicję podpisu elektronicznego oraz jego kwalifikowanej wersji:

---

<sup>56</sup> Na temat prac odnośnie dyrektywy o podpisie elektronicznym zobacz: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 80. Prace te sprowadziły się do dwóch dokumentów: 1. Ensuring Security and Trust in Electronic Communications: towards a European Framework for Digital Signatures and Encryption z 08.10.1997 r., Communication on a European Initiative in Electronic Commerce z 16.04.1997 r. (są one wymienione w preambule dyrektywy o podpisie elektronicznym- pkt (1) i (2)).

<sup>57</sup> Directive 1999/93/EC of the European Parliament and of the Council on 13. December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities z 19.01.2000 r.

<sup>58</sup> Nawiązuje do tego punkt 21 preambuły przewidujący stosowanie podpisów elektronicznych w procedurach prawnych w państwach członkowskich. Prawne uznanie podpisu ma być oparte na obiektywnych kryteriach i nie może się łączyć z autoryzacją certification-service-providers.

<sup>59</sup> Punkt (20): (...) advanced electronic signatures which are created by a secure-signature-creation-device can be regarded as legally equivalent to hand-written signatures only if requirements for hand-written signatures are fulfilled.

- a) podpisem elektronicznym są dane w formie elektronicznej, logicznie powiązane z innymi danymi przesyłanymi w drodze elektronicznej na zasadach, które są równocześnie metodą uwierzytelniania tych danych,
- b) podpis w formie kwalifikowanej to podpis, który spełnia następujące warunki:
- związany jest wyłącznie z podpisującym,
  - umożliwia identyfikację podpisującego,
  - został wygenerowany za pomocą środków będących pod wyłączną kontrolą podpisującego,
  - jest powiązany z innymi danymi w taki sposób, iż zawsze pozwala na wykrycie każdej zmiany danych.

W kolejnych artykułach uregulowano także prawa takie jak dostęp do rynku (art.3), zasady międzynarodowego rynku (art. 4), odpowiedzialności (art. 6). Art. 5 jest o tyle istotny, iż przewiduje zrównanie mocy prawnej podpisu elektronicznego z podpisem własnoręcznym. W punkcie 2 art. 5 zobowiązano państwa członkowskie do zapewnienia, iż podpis elektroniczny nie będzie miał skutków prawnych i nie będzie dopuszczony jako dowód w procedurach prawnych jedynie ze względu na to, że:

- jest w elektronicznej formie,
- nie bazuje na kwalifikowanym certyfikacie,
- nie bazuje na kwalifikowanym certyfikacie wystawionym przez akredytowanego certyfikację-service-provider'a,
- nie został stworzony dzięki uznanym urządzeniom do tworzenia podpisów elektronicznych.

Art. 13 nakłada obowiązek wdrożenia postanowień dyrektywy przez państwa „15” do 19. czerwca 2001 r.

Kończąc rozważania na temat podpisu elektronicznego można stwierdzić, iż dyrektywa z jednej strony zakłada brak monopolu na usługi certyfikacyjne i zachowanie zasad pełnej konkurencyjności na rynku usług, z drugiej zaś gwarantuje dostępność tych usług na poziomie najwyższego zaufania<sup>60</sup>. Nie przesądzono charakteru podpisu, postuluje się zasadę pełnego zaufania do usług związanych z podpisami elektronicznymi, konkurencyjność usług, zasadę pewności podpisu (te same skutki prawne co podpis własnoręczny).

Dyrektywa zakłada ukształtowanie równowagi między bezpieczeństwem interesów podmiotów, które korzystają z usług certyfikacyjnych a zasadami prowadzenia działalności gospodarczej w warunkach rynku opartego na wolnej konkurencji.<sup>61</sup> Dyrektywa poprzez swój zakres stwarza dodatkową gałąź nowej gospodarki (usługi certyfikacyjne) orz zapewnia nową jakość komunikacji. Łączy ona niejako zagadnienie społeczeństwa informacyjnego, elektroniczną gospodarkę oraz prawa autorskie w sieci w jedną spójną całość opartą na zaufaniu i pewności elektronicznych transakcji i przekazie danych.

---

<sup>60</sup> I. Sitnicki, M. Srebrny, *Jak podpisuje się świat*, „Rzeczpospolita” z 09.02.2001 r.

<sup>61</sup> Ibidem.

Przestawione przeze mnie uregulowania unijne w kwestii Internetu wskazują jednoznacznie, iż Zjednoczona Europa staro się doścignąć Stany Zjednoczone w „elektronicznym wyścigu”. Nadrabianie zaległości do największego swego partnera handlowego odbywa się nie tylko na rynku internetowym czy elektronicznym lecz przede wszystkim w kwestii ustawodawstwa.

Europa dostrzegła szansę, która może rozwiązać wspólne problemy (inflacja, bezrobocie) oraz może stworzyć silne podstawy do jeszcze większego zjednoczenia (choćby poprzez Wspólny Rynek). Działania podjęte przez Komisję i inne organy Unii zmierzają właśnie w tym kierunku.

## Rozdział III.

### Zastosowanie Internetu w polskim prawie publicznym

#### 1. Prawo konstytucyjne.

##### Podstawowe prawa i wolności obywatelskie

Dzisiejszy postęp techniczny sprawia, że nie orientujemy się, a wręcz gubimy w coraz to lepszych wynalazkach czy nowinkach ery informatycznej. A cóż dopiero mówić o systemie prawnym nie przygotowanym na e-rewolucję (e-przed słowem oznacza electronic). Bycie *on-line* staje się koniecznością, gdyż elektroniczna gospodarka nigdy nie zasypia. Ogólnie pojęte sieci (telekomunikacyjne, informatyczne) oplatają coraz liczniejsze obszary naszego życia, wkraczają często w sfery dotychczas będące oazą spokoju. Spójrzmy więc czy podstawowe wolności i prawa nie są zagrożone przez Internet.

Konstytucja Rzeczypospolitej Polskiej z 02.04.1997 r. w artykule 14 ustanawia wolność prasy i innych środków masowego przekazu. Polski system prawny definiuje pojęcie prasy (Ustawa z dnia 26.01.1984 r. prawo prasowe art.7 ust.2 pkt 1). Z kolei według orzeczenia Sądu Najwyższego Stanów Zjednoczonych Ameryki z 26.06.1997 r. w sprawie *Reno v. ACLU* Internet to rodzaj prasy odmiennie traktowany niż radio i telewizja.

Widzimy więc, że Internet objęty jest konstytucyjną wolnością przekazu choć w niektórych krajach odmiennie się go klasyfikuje. Z kolei art. 54 Konstytucji mówi o wolności wyrażania swych poglądów oraz pozyskiwania i rozpowszechniania informacji. Informatyczna sieć to dziś najlepszy, najwygodniejszy i najszybszy sposób zdobywania wiedzy na tematy wręcz nieograniczone. Stanowi także formę komunikacji międzyludzkiej (mowa tu m.in. o tzw. forach dyskusyjnych, poczcie elektronicznej czy IRC - *Internet Relay Chat*), to również przesyłanie dźwięku, tekstu i obrazu.

Z wykorzystaniem Internetu wiążą się i problemy. Mowa tu o powszechnie dostępnej pornografii, handlu narkotykami, praniu brudnych pieniędzy w sieciach elektronicznych. Jak pogodzić wolność sieci z wolnością słowa? Jak ustrzec się zjawisk zagrażających moralności nieletnich czy bezpieczeństwu państwa, nie narażając się przy tym na głosy oskarżające o cenzurę i wkraczanie władzy publicznej w sferę wolności obywatelskich? Kwestia ochrony dóbr osobistych innych ludzi jest także gorąca. Jak chronić społeczeństwo przed tego typu zachowaniami? Czy mają to robić dostawcy usług w sieciach (*service providers*)? Czy też specjalnie do tego powołane instytucje? Czy może pozostawić tą kwestię sądom powszechnym?

Inicjatywy mające doprowadzić do „oczyszczenia” sieci mają na celu ograniczenie czy też wyeliminowanie owych zjawisk (przytoczyć tu należy projekt członków Senatu USA J.J. Exona i S. Gortona). Jednak owe przedsięwzięcia zawsze spotykają się ze zdecydowanym oporem środowisk informatycznych. Przeciwnicy cenzury posługują się szeroko rozumianą wolnością słowa. Znamienna jest tu I poprawka do Konstytucji USA, mówiąca o zakazie stanowienia prawa, które

powodowałyby ograniczenie wolności słowa i publikacji. Trudno pogodzić konstytucyjną zasadę wolności słowa i komunikacji z żądaniami, aby przepływ informacji w sieciach poddać kontroli ze strony państwa, zwłaszcza ze względu na ochronę bezpieczeństwa i porządku publicznego<sup>62</sup>. Nie można zaakceptować istnienia stron z dziecięcą pornografią, instrukcjami konstrukcji ładunków wybuchowych czy broni, stron promujących przemoc i organizacje skrajnie politycznie czy społecznie (neofaszyści, ultra narodowcy czy sataniści).

Wydaje się więc, że rozwiązanie tych wszystkich problemów leży w relacji ograniczenia pełnej swobody rozpowszechniania materiałów w sieciach komputerowych do zagwarantowanej w polskiej Konstytucji wolności wyrażania poglądów oraz rozpowszechniania informacji (art.54 ust.1).<sup>63</sup>

Należy też pomyśleć i o tym, iż sam Internet jest siecią globalną, często nie poddającą się ustawodawstwu danego państwa. Zważyć należałoby konieczność ustalenia jednego światowego prawa dotyczącego tych właśnie kwestii. Dużą rolę będą musiały tu odegrać Trybunały Konstytucyjne czy też sądy powszechne poszczególnych państw.

Kolejnym ciekawym problemem jest pozyskiwanie informacji oraz aktywne uczestnictwo obywateli w życiu publicznym. Materię tą regulują art. 54 ust 1, art. 61 i 63 Konstytucji RP. Już teraz internauta, który szuka wiadomości o swych przedstawicielach we władzach czy to państwowych, czy to samorządowych korzysta z Internetu, aby uzyskać interesujące go informacje.

Dane zaprezentowane na konferencji pt. „Miasta w Internecie” (Tarnów 1999 r.) wskazują, że w połowie 1999 roku własne strony WWW miało 715 gmin i 154 powiaty. Dużo do życzenia pozostawiają jednak techniczne opracowania owych witryn. Lecz są także wyjątki. Strony niektórych miast np. Szczecina, Łodzi czy Raszyna pozwalają na znalezienie informacji o pracach władz samorządowych, a w Szczecinie nawet na wnoszenie uwag, do skarbnika gminy dotyczących budżetu miasta (anonimowo, gdyż podanie nazwiska i adresu *e-mail* nie jest obowiązkowe). Trwają prace nad udostępnieniem mieszkańcom miast adresów internetowych urzędników magistratów. Pozwoli to w przyszłości na rozładowanie kolejek w samorządowych urzędach. Z kolei serwisy Raszyna i Szczecina umożliwiają nagranie na dysk niezbędnych formularzy, aby wypełnić je na swoim komputerze-podobna funkcja jest planowana w serwisie łódzkim.<sup>64</sup>

Dziś można też dotrzeć do większości rządowych dokumentów i aktów prawnych dzięki właśnie sieci. Nie trudno sobie wyobrazić sytuację, kiedy każdy kto tylko zapragnie będzie mógł wydrukować interesującą go ustawę w elektronicznej księgarni, czy przejrzeć ją w elektronicznym kiosku w szerszej niż obecnie skali (dziś odbywa się to dzięki drogim programom komputerowym, a dostęp do Internetu nie jest powszechny).

W wielu krajach (m. in. w USA i w Niemczech) istnieje obowiązek ciążyący na organach administracji publicznej posiadania własnych stron WWW. Może w perspektywie kilku lat dzięki Internetowi będziemy mogli w myśl art. 63

---

<sup>62</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.16.

<sup>63</sup> Ibidem.

<sup>64</sup> J. Karolek, *Elektroniczni obywatele*, tygodnik „Wprost” dodatek „Intermedia” z 22.02.2000 r., s. 12-13.

Konstytucji składać petycje, wnioski i skargi w interesie publicznym do organów władzy państwowej i samorządowej.

Doskonałym przykładem jest tu wspomniany serwis miasta Szczecina. Już niedługo będziemy mogli dostarczać zeznania podatkowe w elektronicznej formie do Urzędów Skarbowych, formularze zus-owskie oraz dzięki nowelizacji kodeksu postępowania cywilnego składać pozwycy do sądów powszechnych.<sup>65</sup> Nie są rzadkością elektroniczne konferencje prasowe czy spotkania z internautami mające na celu bliższy kontakt ze społeczeństwem.

Pojawia się jednak trudny na razie do rozwiązania problem dostępu do zaawansowanych technologii. Trwa dyskusja w krajach, które nie są zamożne i nie korzystają z owoców e-rewolucji, jak zniwelować powiększającą się przepaść w komputeryzacji społeczeństw a co za tym idzie także i w dostępie do wiedzy.

To co dotyczy państw ma miejsce także w stosunku do zwykłych obywateli – określanych mianem „analfabetów ery informatycznej” czy też „proletariatu informatycznego”. Kwestia dostępu do sieci jest jednak problemem czysto finansowym, w którym znaczącą rolę gra pieniądz. Pojawiają się postulaty zapewnienia „usług podstawowych” czy też uniwersalnych.

W marcu 2000 r. na szczycie Unii Europejskiej w Lizbonie przygotowano plan działań, mających zmniejszyć internetowy dystans do USA. I tak m.in. Unia proponuje<sup>66</sup>:

-by do 2002 r. zostały stworzone nowe, pojemne łącza telekomunikacyjne, łączące największe ośrodki uniwersyteckie i techniczne;

-aby do 2001 r. wszystkie szkoły w „piętnastce” były podłączone do Internetu, a do 2002 r. wszyscy nauczyciele zostali przeszkoleni z korzystania z sieci.

Polski program „Internet w każdej szkole” zmierza ku zapewnieniu wszystkim szkołom równych szans oraz do otwarcia się młodzieży na świat. Sama waga i doniosłość informatyzacji państwa znalazła odbicie w ostatniej kampanii wyborczej na fotel prezydenta. Hasłem jednego z kandydatów był powszechny dostęp do Internetu.

## E- demokracja

Przełomowe może okazać się użycie Internetu w kampanii wyborczej i w samych wyborach. Dotychczas był on biernie wykorzystywany przy prezentacji kandydatów i ich programów na stronach WWW.

Marcowe prawyborzy 2000 r. w Partii Demokratycznej w stanie Arizona pokazały jak może być on zastosowany w pełni. Liczba oddanych przez sieć głosów była trzy razy większa niż w 1996 r. przy tradycyjnym głosowaniu. Zadecydowały o tym takie czynniki jak:

- brak konieczności udania się do lokalu wyborczego w celu oddania głosu (można powiedzieć, że urna znajdowała się w domu wyborcy),

---

<sup>65</sup> Art. 125 §2 k.p.c..

<sup>66</sup> *eEurope An Information Society For All Communication on a Commision Initiative for the Special European Council of Lisbon 23-24 March 2000*. Zob. więcej na ten temat w rozdziale II poświęconym uregulowaniom w Unii Europejskiej.

- niskie koszty organizacji prawyborów (eliminacja ton papieru, komisji wyborczych czy też zbędność wynajmowania lokali),
  - szybkość transmisji danych i natychmiastowa publikacja wyników.
- Komputery rewolucjonizują także kampanie wyborcze. W jedną noc senator McCain „zebrał” 162 tysiące dolarów poprzez sieć.

Żywy kontakt z elektoratem, który może zadawać pytania i oglądać kandydatów zwiększa atrakcyjność kampanii i poszczególnych osób. Głosujący będą mogli kontrolować stan finansów danego sztabu wyborczego kandydata poprzez sieć (nie mówiąc już o jego stanie majątkowym). W Belgii w wyborach parlamentarnych w 1999 r. próbowano zastosować Internet w głosowaniu. W lokalach wyborczych stały komputery podłączone do sieci. Dodać należy, że i tam także pracuje się nad wyborami w pełni *on line*. Zaostrzyć się jednak może walka polityczna dzięki pomówieniom i oszczerstwom publikowanym na stronach WWW.

Jak widzimy tu także pojawiają się pewne zagrożenia. Wszak 100% społeczeństwa nie korzysta z Internetu i nie jest *on line*. Brak gwarancji bezpieczeństwa takich wyborów i przesyłania danych. Możliwość manipulacji wynikami i głosami jest nieporównywalnie większa.

Socjologowie mówią o zmierzchu demokracji, dzięki właśnie sieci, o przesyłaniu informacji i spadku zainteresowania problemami sprawowania władzy. Jednak możliwość decydowania przez społeczeństwo w elektronicznym referendum przemawia do wyobraźni wielu polityków. To dziś tylko marzenie, które od spełnienia dzieli jedynie krok ku idealnej demokracji.

Internet znalazł już szerokie zastosowanie w badaniach opinii publicznej. Nikt nie podważa ich znaczenia przy ustalaniu modelu kampanii wyborczych czy wpływu na społeczeństwo. Przykładem mogą tu być ostatnie wybory na Prezydenta RP, w trakcie których PBS (sopocka Pracownia Badań Społecznych) współpracowała z operatorem telefonii komórkowej GSM. Przybliżone wyniki wyborów zostały podane tuż po zamknięciu lokali wyborczych i nie odbiegały znacząco od oficjalnych.

## **2.Prawo Karne materialne**

Internet wpływa znacząco na różne gałęzie prawa. Oddziałuje także i na prawo karne. Możliwości sieci stosunkowo szybko zostały zauważone przez przestępców. Pojawiły się nowe formy starych przestępstw a tuż obok nich zjawiska dotąd nieznanne.

Polski ustawodawca w kodeksie karnym z 1997 roku próbował je zdefiniować, ująć w ramy przepisów oraz spenalizować. Jednak rozwój Internetu jest tak gwałtowny, że dziś owe rozwiązania nie wystarczają. Często okazuje się, że nie ma właściwych definicji i orzecznictwa w tych sprawach. Wiąże się to z trudnością ścigania owych przestępstw, ich nowością i niestety z częstym ich niedocenianiem. O ileż głośniejszy jest zwykła kradzież od jej elektronicznej odmiany? Straty ponoszone przez wszystkich użytkowników sieci (czy to indywidualnych czy instytucjonalnych) są jednak dużo, dużo większe.

Nowa jakość porozumiewania się (wszystkich ze wszystkimi) stwarza niebezpieczeństwo ze względu na liczbę potencjalnych ofiar (ocenia się liczbę internautów na kilkaset milionów) oraz na trudność w wykrywaniu przestępstw.

Nieznajomość owego zjawiska powoduje, że przestępczość internetowa rozkwita. Stare i nieprzystosowane do nowych realiów przepisy często zamiast pomagać wręcz utrudniają ściganie elektronicznych przestępców. Konieczne są zmiany. Czasami jednak wystarczy ich nowa interpretacja. Spójrzmy jak wzajemnie na siebie oddziałują owe dwie dziedziny naszego życia – Internet i prawo karne.

## Zagadnienia ogólne i rodzaje przestępstw

Do popełnienia „cyber przestępstwa” konieczny jest sprzęt umożliwiający dostęp do Internetu. Ów sprzęt (komputer czy coraz częściej telefon komórkowy) może być uznany za przedmiot, który służył do dokonania czynu zabronionego. Zastosowanie znajdzie więc przepis art. 44 § 2 k.k. mówiący o przypadku tego typu przedmiotów stanowiących mienie ruchome.

Kolejną ciekawą kwestią jest obowiązek skazanego (art. 72 §1 pkt 7 i 8 k.k.) w postaci zakazu stosownego postępowania (czyli w naszym przypadku z korzystania z komputera czy też z Internetu). Widzimy więc, iż pomimo niedoskonałości przepisów istnieją stosowne instytucje prawa karnego mogące znaleźć odpowiednie zastosowanie w przypadku zderzenia z Internetem.

Istotną kwestią na gruncie prawa karnego jest ustalenie czasu i miejsca popełnienia przestępstwa. Jak rozpatrywać cyber przestępstwo pod tymi względami? Jak umiejscowić czyn zniszczenia danych rozsianych na tysiącach komputerów często znajdujących się w różnych częściach globu? Jak określić czas dokonania przestępstwa, gdy pojawiają się problemy z ustaleniem samego działania? Czy miejscem popełnienia przestępstwa ma być komputer sprawcy czy też ofiary? Przy czym zauważyć należy, że osób poszkodowanych zazwyczaj jest wiele (podobnie jak i sprawców). Na owe pytania w najbliższym czasie będzie musiało odpowiedzieć orzecznictwo i doktryna prawa karnego.

Ogromne problemy stwarza identyfikacja sprawcy przestępstwa oraz przypisanie mu winy. W przypadku tzw. *hackingu* często zdarza się, że „włamywacz” nie ma zamiaru wyrządzenia szkody czy też odniesienia korzyści lecz chce tylko wykazać nieskuteczność wszelkich zabezpieczeń. Ci komputerowi przestępcy zazwyczaj bawią się powodując szkody, wytykając operatorom błędy oraz w pewien sposób poprawiają bezpieczeństwo, ukazując niedostrzegalne luki w oprogramowaniu.<sup>67</sup>

Dobrym przykładem ilustrującym trudność wykrycia przestępcy jest przypadek wirusa „*I love you*”. Pewien Filipińczyk zainfekował miliony komputerów siejąc panikę wśród wszelkich użytkowników sieci. Funkcjonariusze Policji całego cywilizowanego świata zostali postawieni w stan pogotowia. Po wielu tygodniach poszukiwań ustalono jednak kto doprowadził do strat szacowanych na 5-10 mld dolarów.<sup>68</sup>

<sup>67</sup>Porównaj art. A. Adamskiego z P.S. 1998/11-12/149- odmiennie R. Zakrzewski w art. M.Prawn.1998/10/378.

<sup>68</sup>J. Giziński: *Strażnicy sieci*, „Wprost” z dn.21.05.2000r. s. 5- dodatek Intermedia.

Widzimy więc, że kwestie winy i identyfikacji sprawcy są wysoce skomplikowane. Przyjrzyjmy się jednak temu jaki jest zakres potencjalnych podmiotów podlegających odpowiedzialności. A oto ich lista:

1. dysponent (operator) sieci telekomunikacyjnej (zazwyczaj przedsiębiorstwo telekomunikacyjne);
2. dostawca dostępu do sieci (nie ma on wpływu na prezentowane treści);
3. dostawca zawartości sieci;
4. dostawca usług w sieciach(np. dostawca dodatkowych usług);
5. użytkownik końcowy.

**Ad.1.** Operator sieci nie odpowiada za prezentowane materiały. Nie ma podstaw do jego odpowiedzialności karnej.

**Ad.2.** I tutaj tak jak i w pierwszym przypadku brak przepisów dotyczących odpowiedzialności karnej.

**Ad.3.** Powszechnie przyjmuje się, że podmioty te podlegają odpowiedzialności karnej za udostępnianie przez sieci komputerowe własnych materiałów.<sup>69</sup>

**Ad.4.** Największy problem wyłania się przy tym podmiocie. Nie podlega dyskusji jego odpowiedzialność przy prezentowaniu własnych danych. Lecz odmiennie należy podejść do sytuacji, w której *service provider* udostępnia odpowiednie środki techniczne, bądź też pośredniczy w rozpowszechnianiu materiałów innych osób. Taką działalność można zakwalifikować jako pomocnictwo.

**Ad.5.** Użytkownik końcowy ponosi pełną odpowiedzialność za prezentowane przez siebie treści.

Wydaje się, iż największym wyzwaniem jest sprecyzowanie odpowiedzialności za zaniechanie. Aby jednak postawić zarzut wskazać należy prawny obowiązek działania. Ze względu na brak potrzebnego przepisu należy stwierdzić, że jest to niemożliwe. Trudne do wyobrażenia jest także kontrolowanie milionów stron i informacji przechodzących przez dany serwer. To właściwie fizycznie niewykonalne. Należy zastanowić się nad wprowadzeniem regulacji dotyczącej określonego zachowania czy też pozyskiwania informacji o prezentowanych przez *providera* zakazanych treściach. Spróbujmy dokonać pewnego ogólnego podziału przestępstw komputerowych.

Komitet Ekspertów Rady Europy<sup>70</sup> w latach '80 postulował, aby uznać za przestępstwa komputerowe następujące czyny:

- oszustwa związane z wykorzystaniem Internetu,
- fałszerstwa komputerowe,
- niszczenie danych lub programów komputerowych,
- sabotaż komputerowy,
- nieuprawnione wejście do systemu,
- podsłuch komputerowy,
- bezprawne kopiowanie, rozpowszechnianie lub publikowanie programu komputerowego prawnie chronionego.

<sup>69</sup> Odmiennie w sprawie Felixa Somma- wyrok sądu karnego w Monachium dostępny na stronie [www.kuner.com](http://www.kuner.com)

<sup>70</sup> Computer- Related Crime: Recommendation No.R(89)9 on the computer related crime and final report of the European Committee on Crime Problems. Council of Europa, Strasbourg 1990.

Opublikowano także i drugą listę, na której znalazły się przestępstwa o mniejszym stopniu szkodliwości i niewymagające ścisłej współpracy międzynarodowej w zakresie ścigania i jurysdykcji. Oto one:

- modyfikacja danych lub programów komputerowych
- szpiegostwo komputerowe
- używanie komputera bez upoważnienia i zezwolenia.

Z kolei Interpol przestępstwa komputerowe definiuje jako przestępstwa w zakresie techniki komputerowej i dzieli je na:

1. Naruszanie praw dostępu do zasobów, a w szczególności:
  - *hacking*, czyli nieupoważnione wejście do systemu informatycznego
  - przechwytywanie danych,
  - kradzież czasu, czyli korzystanie z systemu poza wyznaczonymi godzinami,
  - modyfikacja zasobów przy pomocy bomby logicznej, konia trojańskiego, wirusa czy robaka komputerowego.
2. Oszustwa przy użyciu komputera a w szczególności:
  - oszustwo bankomatowe,
  - fałszowanie urządzeń wejścia i wyjścia,
  - oszustwo na maszynach do gier,
  - oszustwo poprzez podanie fałszywych danych identyfikacyjnych,
  - oszustwo w systemie telekomunikacyjnym.
3. Powielanie programów w tym:
  - gier we wszystkich postaciach,
  - innych programów komputerowych,
  - topografii układów scalonych.
4. Sabotaż zarówno sprzętu jak i oprogramowania.
5. Przechowywanie zabronionych prawem zbiorów.
6. Przestępstwa popełnione w sieci.

Pomimo osobnego wydzielenia przestępstw dokonanych w sieci należy zwrócić uwagę, że wskutek postępującej informatyzacji i dostępu do Internetu wszystkie te przestępstwa można popełnić właśnie poprzez Internet.<sup>71</sup>

## Pornografia w Internecie

Najczęściej w cyberprzestrzeni spotykamy się z treściami pornograficznymi. Trudno nawet w przybliżeniu podać liczbę stron i materiałów pornograficznych dostępnych w sieci. Zjawisko to, niemożliwe do ścisłego określenia, stanowi dziś nie lada wyzwanie tak dla ustawodawców jak i organów ścigania.

Znane są już uzależnienia od sieciowej pornografii. Zdaniem Ala Coopera z Sexuality and Martial Centre w San Jose w samych Stanach Zjednoczonych jest już 200 tysięcy „pornomaniaków”. Za osoby uzależnione All Cooper uznał te wszystkie, które spędzają na przeglądaniu „informatycznych świerszczyków” więcej niż 11 godzin tygodniowo<sup>72</sup>.

---

<sup>71</sup> A. Adamski, *Przestępstwa komputerowe w nowym kodeksie karnym*, [w:] *Nowa kodyfikacja karna. Kodeks Karny, krótkie komentarze*. Zeszyt 17, Warszawa 1998. Ministerstwo Sprawiedliwości Departament Kształcenia Kadr.

<sup>72</sup> P. Kościelniak, *Zamiast kaset i kompaktów*, „Rzeczpospolita” z 16.03.2000 r.

Dane te pochodzą z 1998 roku, więc zjawisko to widzimy w wyblakłym już świetle. Należy przypomnieć, iż rok internetowy – rozwoju Internetu- to siedem lat zwykłych. Postęp w tej dziedzinie jest więc bardzo szybki.

Spójrzmy jednak jak pornografię penalizuje polski ustawodawca w kodeksie karnym. Artykuł 202 §1 k.k. kryminalizuje publiczne prezentowanie treści pornograficznych w taki sposób, że może to narzucić ich odbiór osobie, która tego sobie nie życzy<sup>73</sup>. Jest to więc przyjęcie koncepcji „wolności od” kontaktu z treściami pornograficznymi. Zatem rozpowszechnianie pornografii wśród osób dorosłych, które sobie tego życzą nie jest przestępstwem. Mowa tu oczywiście o miękkiej odmianie zjawiska. Skoro jest miękka pornografia więc występuje także i twarda.

Jak polski ustawodawca reguluje z kolei tą kwestię? Paragraf 3 artykułu 202 k.k. wskazuje co należy rozumieć jako ową odmianę. To „treści pornograficzne z udziałem małoletniego poniżej lat 15 albo związane z użyciem przemocy lub posługiwaniem się zwierzędem”. Sankcja karna w przypadku produkcji, rozpowszechniania lub sprowadzania owych treści, to kara pozbawienia wolności od 3 miesięcy do lat 5. Doktryna zauważa niekonsekwencję k.k., który traktuje „jako twardą pornografię treści pornograficzne związane z posługiwaniem się zwierzędem lecz sodomia jako taka nie jest w Polsce przestępstwem”<sup>74</sup>.

Ważny, z punktu widzenia tematu Internetu, jest § 2 art.202. „Kto małoletniemu poniżej lat 15 prezentuje treści pornograficzne lub udostępnia mu przedmioty mające taki charakter podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.” Ponieważ przepis ten zabrania jakiegokolwiek prezentowania treści pornograficznych małoletniemu w formie umyślnej (czyli w postaci zamiaru bezpośredniego albo ewentualnego) należy zastanowić się nad istnieniem po stronie osoby prezentującej owego zamiaru.<sup>75</sup>

Użycie przez ustawodawcę w art. 202 nowego k.k. pojęcia „treści pornograficzne” nie pozostawia wątpliwości, iż jego wolą było objęcie zakazem rozpowszechniania również treści pornograficznych przenoszonych za pomocą elektronicznego przekazu danych<sup>76</sup>. Pamiętajmy jednak o tym, iż prezentowanie tzw. pornografii miękkiej penalizowane jest tylko wtedy, gdy ktoś się z nią styka nie życząc sobie tego.

Według ekspertów największym problemem jest pedofilia w sieci<sup>77</sup>. Internet to wymarzone narzędzie dla wielu pedofilów. Cyberprzestrzeń zapewnia anonimowość, więc czują się tam bezpiecznie. Transfer danych pozwala unikać kontroli granicznych. W państwach biedniejszych nie jest problemem „za deskorolkę” uzyskać zgodę dziecka na kilka zdjęć czy też „odegranie małej rólki w filmie”.

Seks-turystyka jest dużym zagrożeniem, ale i jednocześnie dochodowym interesem, który został opanowany przez zorganizowane grupy przestępcze.

---

<sup>73</sup> L. Gardocki, *Prawo karne*, Warszawa 1998, s.248.

<sup>74</sup> Ibidem, s. 249.

<sup>75</sup> J. Dzierżanowska, M. Wąsek-Wiaderek, *Prawo karne a Internet- wybrane zagadnienia*, [w:] R. Skubisz (red): *Internet – problemy prawne*, Lublin 1999, s.251.

<sup>76</sup> M.Filar, *Przestępstwa seksualne w nowym KK*. [w:] *Nowa kodyfikacja karna. Krótkie komentarze*, Warszawa 1997, s.39.

<sup>77</sup> M.in. Christ Dannerman z niemieckiej grupy Tenre des Hommes i Ron O’Grady z organizacji End Child Prostitution in Asian Tourism.- P. Kościelniak, *Porno problem*, „Rzeczpospolita”, 16.03.2000 r.

Zjawiska te przybierają niepokojące rozmiary. Podam tu przykład akcji Scotland Yardu, w wyniku której aresztowano Adriana Leish'a – 45 letniego księdza z Gilesgate w Zjednoczonym Królestwie. W jego komputerze znaleziono 8998 plików, z których każdy zawierał do 15 zdjęć pornograficznych. Ksiądz posługiwał się do transmisji danych systemem, który uniemożliwiał odczytywanie jego korespondencji. Wymieniał się materiałami pornograficznymi z innymi pedofilami.<sup>78</sup> Przyznać więc trzeba, że zjawisko to wręcz zastrasza. Ciekawa kwestia pojawia się w przypadku komputerowego generowania pornografii przy pomocy najnowszej techniki animacji. Odpada tu aksjologiczna przesłanka penalizacji. Dzieci bowiem nie są krzywdzone. Również i ten problem należałoby w przyszłości uregulować.<sup>79</sup>

Pornografia w sieci to także sposób popełniania innych przestępstw. Mowa tu o oszustwach wykorzystujących naiwność „erotycznych turystów”. Wyłudzenie numerów kart kredytowych i obciążanie rachunków internautów nie jest rzadkie. Przykładem może tu być skarga FTC przeciw nowojorskiej firmie Crescent Publishing Group do sądu w Nowym Yorku. Firma ta wyłudziła od swoich internetowych klientów 188 milionów dolarów<sup>80</sup>. Sumę wręcz niebotyczną. Także i takie liczby ukazują skalę zjawiska „porno biznesu” w sieci.

Ponad połowa stron WWW pochodzi ze Stanów Zjednoczonych- ojczyzny Internetu. Dla porównania zobaczymy więc jak ten kraj normuje kwestię pornografii. Ustawodawstwo federalne rozróżnia pojęcia „nieprzyzwoity” (*indecent*) i „obsceniczny” (*obscene*).<sup>81</sup> Prezentowanie treści nieprzyzwoitych jest dozwolone i korzysta z ochrony Pierwszej Poprawki do Konstytucji USA. Jednakże treści obsceniczne nie są objęte już tą ochroną, chociaż w jednym z orzeczeń Sądu najwyższego USA posiadanie owych materiałów we własnym domu „z wyłączeniem treści pornografii dziecięcej” uznane zostało za dozwolone<sup>82</sup>. Duże znaczenie ma amerykańska ustawa o telekomunikacji (The Telecommunication Act) z 1996 roku. W art. 48 §223(a) zawarty jest zakaz umyślnego elektronicznego przekazywania treści obscenicznych i nieprzyzwoitych odbiorcom poniżej 18 roku życia, jak również umyślnego zezwolenia na użycie urządzeń znajdujących się pod kontrolą danej osoby dla dokonania przekazu o takiej treści<sup>83</sup>. Zaś §223(d) penalizuje umyślne przesyłanie lub pokazywanie, za pomocą interaktywnych usług komputerowych, osobom poniżej 18 roku życia treści dotyczących aktywności seksualnej lub narządów płciowych w sposób oczywiście obraźliwy w rozumieniu standardów przyjętych we współczesnym społeczeństwie.

Widzimy więc, że uregulowanie amerykańskie ma poszerzony zakres ochrony podmiotowej (podniesiona granica wieku, w Polsce – poniżej 15 roku życia) oraz bardziej szczegółowe przepisy dotyczące Internetu , tu określonego mianem interaktywnych usług komputerowych.

---

<sup>78</sup> M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, s.12, dokument dostępny w Internecie na serwerze [www.vagla.eu.org](http://www.vagla.eu.org)

<sup>79</sup>Ibidem, s. 11.

<sup>80</sup> Z. Domaszewicz, *Plamy w sieci*, „Gazeta Wyborcza” z dn. 15.09.2000, s. 26-28.

<sup>81</sup> Sprawa Miller v. California, (413.US.15(1973))

<sup>82</sup> Sprawa Stanley v. Gorgia; por. Y.Akdeniz, *Pornography on the Internet*, praca dostępna w Internecie na stronach [http://elj.warwick.ac.uk/jilt/Internet/97\\_lakokz/](http://elj.warwick.ac.uk/jilt/Internet/97_lakokz/)

<sup>83</sup> J. Dzierżanowska, M. Wąsek-Wiaderek, *Prawo karne a Internet- wybrane zagadnienia*, [w:]R. Skubisz (red.): *Internet- problemy prawne*, Lublin 1999, s.246.

Podsumowując problem pornografii w sieci dostrzec należy skalę tego zjawiska jak również jego ewolucję, która próbuje ominąć przepisy ustawowe. Uwagę zwraca także to, iż prawie we wszystkich krajach twarde pornografia (m.in. pedofilia) jest zakazana. Pozostaje nierozwiązana kwestia ścigania owego przestępstwa przez państwowe organy ścigania.

## *Hacking*

Przejdźmy teraz do najczęściej popełnianego, wyrządzającego największe straty<sup>84</sup>, przestępstwa – do *hackingu*.

Skąd wzięło się to słowo? Jakie jest jego etymologiczne pochodzenie? Otóż oznaczało ono człowieka ciężko pracującego. Tak też zwano pierwszych cybermaniaków, spędzających przy komputerach całe tygodnie. Później zaczęto tak nazywać komputerowego włamywacza, gdyż wykorzystywał on swą wiedzę nabytą, dzięki tysiącom godzin praktyki. Dziś utrzymało się znaczenie słowa *hacker* – jako kogoś kto pokonuje zabezpieczenia – kody i hasła – broniące dostępu do systemu operatora.<sup>85</sup>

Polski k.k. penalizuje przestępstwo *hackingu* w art.267 §1. Jest to elektroniczna forma bezprawnego uzyskiwania informacji zagrożona karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. Na gruncie art.267 § 1 k.k. należy stwierdzić, że przełamanie magnetycznego albo innego zabezpieczenia następuje z chwilą dokonania czynu wpływającego na działanie owego zabezpieczenia. Nie jest więc objęte przepisem samo podłączenie się do sieci teleinformatycznej, gdyż nie stanowi ono przełamania kodu lub hasła i jest niezbędne do uzyskania jakichkolwiek danych.

Sporne jest natomiast w doktrynie wykorzystywanie przez *hackerów* tzw. dziur w konfiguracji czy oprogramowaniu systemowym. Czy takie zachowanie spełnia przesłanki art.267 §1 k.k. czy też nie? Wszak bezpośrednio nie ma tu przełamania zabezpieczenia lecz wykorzystanie czyjegoś błędu<sup>86</sup>. R. Zakrzewski uważa jednak odwrotnie, uzależniając przestępcze działanie od samego zapoznania się z treścią nie przeznaczoną dla *hackera* informacji.<sup>87</sup>

Właśnie kwestia zapoznania się przez nieuprawnioną osobę z informacją stwarza dużo kłopotów. Kodeksy karne z 1969 (art. 172 §1) i z 1932 r. (art.253 §1) do naruszenia poufności informacji nie wymagały zapoznania się z ich treścią. Już samo przełamanie zabezpieczeń było karalne. Ustawodawca jednak w art.267 §1 k.k. zawarł owe sformułowanie co nie wydaje się rozwiązaniem trafnym. Stwarza natomiast wiele problemów w kwestii ustalenia czy sprawca faktycznie zapoznał się z materiałami w sieci, do których nie był uprawniony.

Często *hackerzy* dokonują włamań elektronicznych tylko po to, aby się sprawdzić (potrenować) czy też wykazać błędy operatorowi w zastosowanych przez niego zabezpieczeniach. Sporne jest także czy do zakwalifikowania czynu zabronionego z art.267 §1 k.k. wystarczy samo uzyskanie hasła dostępu czy też

---

<sup>84</sup> Według szacunków FBI straty te wynoszą około 7,5 mld dolarów rocznie, dane na serwerze <http://www.iss.net>.

<sup>85</sup> Na przestępcze działanie *hackera* narażone są właściwie wszystkie komputery i urządzenia (telefony komórkowe także nie są bezpieczne)..

<sup>86</sup> A. Adamski: art. PS/1998/11-12/149.

<sup>87</sup> R. Zakrzewski: art. M.Prawn. 1998/10/378.

konieczny jest ten drugi krok przestępnego wejścia do systemu i zapoznanie się z informacjami.

Paragraf 2 art. 267 k.k. penalizuje samo zakładanie czy posługiwanie się urządzeniami podsłuchowymi, wizualnymi albo innymi urządzeniami specjalnymi w celu pozyskania informacji. Nie ma wątpliwości, że do takich urządzeń zaliczyć można komputer osobisty (PC- *Personal Computer*).

Podsłuch komputerowy, bo to właśnie zjawisko kryminalizuje §2 art. 267 k.k., można podzielić na 2 grupy:

- na analizę fal elektromagnetycznych emitowanych przez sprzęt komputerowy. Ponieważ każde urządzenie generuje promieniowanie a uzyskując jego obraz można dokonać odtworzenia informacji dlatego też metoda ta jest wykorzystywana nawet na odległość od 300 do 1000 metrów.<sup>88</sup>

- i przechwytywanie danych z transmisji teleinformatycznych.

*Hackerzy* w celu uzyskania danych posługują się technikami, które nie naruszają zabezpieczeń. Są to :

- *sniffing* – „wąchacz” czyli podsłuchiwanie pakietów pomiędzy komputerami,

- *IP spoofing* – istnieje kilka odmian, ale przede wszystkim oznacza to podszywanie się pod inny komputer,

- *session hijacking*,

- *fragmentacja-reasemblacja pakietów*,

- i wspomniane już wykrycie luki (*bug*).

Wprowadzenie, więc innej osoby w błąd poprzez posługiwanie się komputerem nie spełnia przesłanek art. 267 § 1i2 k.k. Widzimy więc, jak szybko *hackerzy* znajdują sposoby omijania prawa i jak szybko owe przepisy się dewalują i nie nadążają za zmianami w informatyce.

Inne programy, którymi posługują się *hackerzy* to:

- „*koń trojański*”,

- „*back door*”,

- „*exploit*”.

W samym środowisku komputerowych włamywaczy następuje specjalizacja. Pojawili się już *crackerzy* (uzyskują korzyści materialne z przestępstwa) oraz *phraekerzy*, którzy przełamują zabezpieczenia systemów telekomunikacyjnych.

Kolejnym przepisem dotyczącym ochrony informacji jest art. 268 §2 k.k. To kwalifikowana forma przestępstwa udaremnienia uzyskania informacji. Ochroną omawianych przepisów (267 i 268 k.k.) objęta jest wszelka korespondencja osób fizycznych, prawnych, organizacji i instytucji, prowadzona w formie pisemnej, ustnej, telegraficznej i telefonicznej.<sup>89</sup> Należy tu sprecyzować stwierdzenie „zapisu na komputerowym nośniku informacji, które zawarte jest w § 2 art. 268 k.k.. Niestety, ale nigdzie nie znajdziemy definicji ustawowej owego wyrażenia. Ustawodawca w różnych aktach normatywnych (ustawa o rachunkowości, w Prawie Bankowym czy Kodeksie Karnym Skarbowym<sup>90</sup>) mówi o „komputerowym

<sup>88</sup> K.B. Urbański, *Chroń swój komputer*, „Rzeczpospolita” z dn.15.05.2000 r.

<sup>89</sup> R. Zakrzewski: art. w M.Prawn. 1998/10/378.

<sup>90</sup> Ustawa o rachunkowości z dn. 29.09.1994r (Dz.U.94121.591), Prawo bankowe z dn. 29.08.1997r (Dz. U. 97.140.939), k.k.s. z dn. 10.09.1999r. (Dz.U.99.83.930).

nośniku danych, elektronicznym nośniku informacji czy nośniku do zapisu informacji w postaci cyfrowej lub na taśmie elektromagnetycznej jak również na elektronicznym nośniku danych”.

Wprawdzie karalne jest oddziaływanie fizyczne, mechaniczne, chemiczne czy magnetyczne na nośniki informacji w celu jego zniszczenia bądź uszkodzenia, lecz należy stwierdzić, że największe znaczenie ma tutaj postać przestępstwa komputerowego (sieciowego). Wprowadzenie do systemów przeróżnych programów komputerowych może wyrządzić nieobliczalne szkody, np. unieruchomienie samolotu będącego w trakcie lotu, dezorganizację pracy szpitala, czy utratę danych z kilkuletnich badań naukowych.

Właśnie ze względu na wyrządzone szkody słusznie ustawodawca podwyższa sankcję w art. 268 §2 i 3 k.k. w porównaniu z typem podstawowym określonym w §1. Ograniczeniem jest tu jednak to, że wszystkie te czyny zabronione są przestępstwami umyślnymi<sup>91</sup>. Oznacza to brak możliwości pociągnięcia do odpowiedzialności karnej za spowodowanie często znacznych strat (na skutek niezachowania elementarnych zasad ostrożności) nawet tych kategorii osób, które mają obowiązek dbania o bezpieczeństwo zasobów informatycznych np. administratorów sieci.<sup>92</sup> W przypadku słabej „kultury informatycznej” wielu urzędników instytucje państwowe czy samorządowe są narażone na poważne straty.

Art. 268 §2 k.k. dotyczy nie tylko niszczenia, usuwania czy zmiany informacji. Dotyka także kwestii uniemożliwienia dostępu do niej uprawnionym użytkownikom. Zjawisko tzw. *mailbombingu*- czyli wysyłania pod wskazany adres tysięcy plików unieruchamiających serwer- stało się głośne w lutym 2000r. po zaatakowaniu przez *hackerów* przedsiębiorstw internetowych (m.in. Yahoo, E-Bay, Amazon.com, CNN, Buy.com, E\*Trade). Wywołując spadek cen akcji tych firm na giełdzie oraz straty w wysokości milionów dolarów.<sup>93</sup>

Kwalifikowaną formą przestępstwa niszczenia, uszkodzenia, usuwania czy zmiany informacji jest przestępstwo z art. 269. Dotyczy ono zapisów o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej. Karą za dokonanie owego przestępstwa jest pozbawienie wolności od 6 miesięcy do lat 8. Karalny jest tu już sam atak na taki zapis informacji lub proces automatycznego jej gromadzenia lub przekazywania.

Nie wymaga więc ustawodawca do zaistnienia tego przestępstwa skutku. Nie jest także konieczne udaremnienie lub znaczne utrudnienie jej dyspozytorowi zapoznanie się z informacją<sup>94</sup>. Negatywnie należy ocenić rozróżnienie ochrony materialnej ze względu na rodzaj podmiotu. Jest to wbrew zaleceniu Komisji Ekspertów Rady Europy<sup>95</sup>. Komisja zwracała uwagę na całościową ochronę bez żadnych preferencji grupowej podmiotów.

<sup>91</sup> W trybie kwalifikowanym § 3 nieumyślność dotyczy tylko znacznej szkody majątkowej.

<sup>92</sup> M. Kliś, T. Martuszek, *Przestępstwa elektroniczne*, tekst dostępny na serwerze [www.vagla.eu.org](http://www.vagla.eu.org)

<sup>93</sup> T. Świderek, *Mniej odwiedzających mniej pieniędzy*, „Rzeczpospolita” z dn.11.02.2000r. i A. Jermiołowski, *Sieciowy terroryzm*, „Rzeczpospolita” z dn. 10.02.2000r.

<sup>94</sup> M. Kliś, T. Martuszek, *Przestępstwa elektroniczne*, op. cit, s.6.

<sup>95</sup> Patrz przypis nr 9.

## Kradzież programu komputerowego i oszustwa komputerowe

W zakresie przestępstw komputerowych możemy znaleźć również kradzież programu komputerowego- art.278 §2 k.k. tzw. piractwo komputerowe. Program sam w sobie nie jest rzeczą, stąd też to uregulowanie znajduje się w oddzielnym przepisie. Przedmiotem ochrony przestępstwa z art.278 §2 k.k. są majątkowe prawa autorskie jego twórcy jak i nabywcy<sup>96</sup>. Unormowane jest to także w ustawie o prawie autorskim i prawach pokrewnych<sup>97</sup>. Do podstawowych form piractwa komputerowego zaliczymy:

- wykonywanie dodatkowych kopii,
- naruszanie treści licencji,
- wykorzystywanie bez zgody właściciela kodu programu do tworzenia nowego,
- nielegalne powielanie i sprzedaż oprogramowania chronionego prawem.

Należy także odnieść wskazane formy przestępstwa kradzieży do przepisu 293 §1 k.k. Dotyczy on paserstwa programu komputerowego, co jest związane z jego nielegalnym uzyskaniem- czyli piractwem komputerowym. Przestępstwa te (kradzież jak i paserstwo) są szczególnie groźne, gdyż nie chodzi tu tylko o indywidualnych „złodziei czy paserów” lecz przede wszystkim zorganizowanych grup przestępczych czerpiących z tego procederu krociowe zyski kosztem prawowitych właścicieli – autorów oprogramowania<sup>98</sup>.

Materię oszustw komputerowych regulują następujące przepisy art. 285, art. 287 i art.311 k.k.. Dodatkowo można zauważyć, że odpowiednie zastosowanie do oszustwa mają artykuły 297 i 298 k.k. Przestępstwo oszustwa komputerowego jest stosunkowo młode. Fakt, że polski ustawodawca w nowym kodeksie karnym z 1997 roku wyodrębnił także tę formę wskazuje na rozwój informatyki, a co za tym idzie również i przestępstw elektronicznych.

Przy klasycznym oszustwie przestępca wprowadza w błąd inną osobę. W oszustwie komputerowym wprowadzona w błąd jest maszyna. Mimo podobieństwa obu przestępstw zauważyć należy rzucające się w oczy różnice. Otóż przy oszustwie z art.286 k.k. działanie polega na osiągnięciu korzyści majątkowej. Jest to przestępstwo materialne i do jego zaistnienia konieczne jest „niekorzystne rozporządzenie własnym lub cudzym mieniem”. Z kolei art. 287 k.k. poszerza zakres czynu zabronionego wprowadzając także „działanie w celu wyrządzenia szkody innej osobie”. Dokonanie oszustwa komputerowego następuje już w chwili „wpłynięcia na automatyczne gromadzenie lub przesyłanie informacji lub zmianę, usunięcie albo wprowadzenie nowego zapisu na komputerowym nośniku informacji”. Widzimy więc, że skutek, w postaci korzyści majątkowej czy szkody, nie jest niezbędny.

Doktryna wyróżnia trzy typy oszustwa komputerowego:

- manipulacja danymi wprowadzonymi do komputera (*input manipulation*),

<sup>96</sup> M. Kliś, T. Martuszek, *Przestępstwa elektroniczne*, op. cit, s. 7.

<sup>97</sup> Art.115, 116 i 117 ustawy o prawie autorskim i prawach pokrewnych z dn.04.02.1994r.Dz.U.00.80.904-j.t.

<sup>98</sup>Na świecie 36% oprogramowania do PC-tów ma nielegalne pochodzenie, a w Polsce około 60%. Zb. Zwiechrzykowski, *Rozkradana informatyka*, „Rzeczpospolita” z 26.05.2000r.

- manipulacja programem (*program manipulation*),
- manipulacja wynikiem (*output manipulation*).

Pierwszy z nich polega na wprowadzeniu fałszywych danych do systemu w celu osiągnięcia korzyści majątkowej. Jest to najpowszechniejsza forma oszustwa, gdyż nie wymaga od przestępcy szczególnych umiejętności i wiedzy. Najbardziej narażone na tego rodzaju działanie są banki i inne instytucje finansowe.<sup>99</sup> Druga forma to przygotowanie programu lub jego modyfikacja w ten sposób, aby działał on wbrew woli operatora lecz po myśli przestępcy. Najczęstszym przypadkiem tego typu jest metoda salami. Polega ona na zmniejszaniu tysięcy rachunków o drobne kwoty (rzędu kilku lub kilkunastu groszy) i przesyłanie ich na uprzywilejowany rachunek. Klienci banków nie zauważają tego procederu, gdyż chodzi tu o „śmieszne sumy”. Lecz w przypadku wielu oszukanych kwoty te sięgają milionów dolarów. Ponieważ przestępstwo to jest trudne do przeprowadzenia i wymaga dobrej znajomości systemu i rozległej wiedzy informatycznej najczęściej popełniane jest przez bankowych informatyków.

Manipulacja wynikiem zwana jest także manipulacją urządzeniami wyjściowymi. Takimi urządzeniami są np. bankomaty i automaty do gry. Nie jest to przestępstwo częste aczkolwiek wykazuje duży wskaźnik dynamiki ze względu na upowszechnianie się tego typu urządzeń oraz coraz łatwiejszy do nich dostęp. Polegać może ono także na wystawieniu fałszywego rachunku (faktury) przy pomocy komputera.

Ustawodawca w art. 285 k.k. zawarł nowy typ przestępstwa - kradzież impulsów telefonicznych. Chociaż przepis tworzony był z myślą o mechanicznym podłączeniu do urządzenia telekomunikacyjnego i uruchomieniu na cudzy rachunek impulsów, to postęp techniczny sprawił, iż przepis dotyczy także cyberprzestrzeni. Podłączenie się do sieci telekomunikacyjnej przez Internet możliwe jest dzięki postępującej informatyzacji telekomunikacji.

Mowa już była o *hackerach*, którzy specjalizują się w łamaniu zabezpieczeń operatorów telekomunikacji. Tak zwani *phreakerzy* znajdują sposoby na obchodzenie już przestarzałego przepisu z art. 285 k.k. Urządzenie zwane *black box* powoduje niewykrycie przez operatora numeru telefonu, przy którym jest ono zamontowane, a dodatkowo sprawia, że „dzwoniący” nie tylko nie płaci za usługę lecz także nie odpowiada na podstawie art. 285 k.k z przyczyny nie uruchomienia impulsów telefonicznych. Zauważmy jednak, że wraz z coraz większą informatyzacją telekomunikacji będzie można przypisać takim zachowaniom znamiona czynu z art. 287 k.k. (oszustwo komputerowe). Zwróćmy uwagę na wyodrębnienie przestępstwa kradzieży impulsów od, czy to zwykłego oszustwa, czy od oszustwa komputerowego, zauważyć należy, że intencje ustawodawcy były odmienne.

W grupie oszustw komputerowych pozwoliłem sobie umieścić także przestępstwo z art. 311 k.k. Choć zawarte zostało ono w Rozdziale XXXVII k.k. pt. „Przestępstwa przeciwko obrotowi pieniędzmi i papierami wartościowymi” to mimo wszystko dzięki sieci można traktować je jako pewnego rodzaju oszustwo

<sup>99</sup> Szacuje się, że w przypadku klasycznego napadu na bank traci on około 8000 dolarów, gdy w przypadku oszustwa komputerowego to strata w wysokości 0,5 mln., K.J. Jakubski, *Przestępczość komputerowa- próba zdefiniowania zjawiska*, [w:] R. Skubisz (red), *Internet- problemy prawne*, op. cit. s. 267.

komputerowe. Giełdy papierów wartościowych już teraz w dużej mierze opierają się na elektronice. Składanie zleceń, system notowań czy informacje giełdowe prowadzone są właśnie w takiej formie.

Dzięki Internetowi przesyłanie informacji do milionów osób czy instytucji nie jest już problemem. Sąd w Melbourne w Australii ostatnio skazał na 2 lata pozbawienia wolności informatyka za rozpowszechnianie fałszywych informacji, mających wpływ na notowania kilku spółek giełdowych. Jest to pierwszy taki wyrok na świecie, a z uwagi na efekt globalizacji, który postępuje szybciej dzięki Internetowi, można przypuszczać, że tego typu orzeczenia będą częstsze. Steven Hourmouzis dzięki wysłaniu 4 milionów *e-maili* znacząco wpłynął na kursy spółek. Efektem owej operacji było 10 tysięcy dolarów. Tylko skuteczna akcja służb dochodzeniowych amerykańskiej i australijskiej giełdy sprawiła, że straty (czy też zyski - w tym przypadku Hourmouzisa) nie były większe.<sup>100</sup>

Kolejnym przykładem skali tego zjawiska jest fakt, iż amerykańska SEC wszczęła postępowania w 15 sprawach związanych z manipulowaniem kursami akcji poprzez Internet. Tu też można zaobserwować udział w tego rodzaju przedsięwzięciach grup przestępczych. Połączenie informatyki i dużego kapitału (nielegalnego) może rodzić poważne komplikacje.

Oszustwo komputerowe dotyka przede wszystkim banki i instytucje ubezpieczeniowe. Należałoby zastanowić się nad wzajemnym stosunkiem art. 297 i 298 oraz at. 287 k.k. Jaka jest więc relacja oszustwa bankowego i ubezpieczeniowego do oszustwa komputerowego? Z uwagi na regulację kodeksową dotyczącą zbiegu przepisów ustawy (art. 11k.k.) należy dojść do wniosku, że czyn wypełniający znamiona obu (czy też wszystkich trzech) przestępstw karany by był w związku z przepisem art. 11 §3 k.k.

Widzimy więc, że przestępstwa komputerowe dotyczą wielu dziedzin życia wypełniając często znamiona kilku przestępstw.

Poza przestępstwami typowymi dla środowiska Internetu (*hacking*, oszustwo komputerowe) możemy wyróżnić wiele czynów, które dzięki sieci nabierają nowego wyrazu. Często także sam komputer podłączony do cyberprzestrzeni staje się narzędziem zabronionego działania. Internet umożliwia porozumiewanie się między ludźmi. Nie zapominajmy jednak i o funkcji sterowania poprzez sieć maszynami. Coraz więcej urządzeń jest dostosowanych do współdziałania z siecią. W przyszłości będzie możliwe porozumiewanie się samych maszyn bez udziału człowieka (już w pewien sposób jest to wykorzystywane np. system EDI).

## Inne przestępstwa

Spójrzmy na tradycyjne przestępstwa, które dzięki sieci uzyskują nowe oblicze. Ze względu na rozległość zagadnienia przedstawię tylko te najbardziej charakterystyczne, wymieniając natomiast pozostałe.

Nie ulega wątpliwości, iż w cyberprzestrzeni zadomowiły się związki przestępcze oraz przeróżne skrajne organizacje. Kwitnie w sieci handel narkotykami. Pojawiły się nawet sklepy oferujące zarówno „towar” jak i informacje o uprawie, hodowli i pozyskiwaniu narkotyków. Dużym problemem jest kwestia

---

<sup>100</sup> Informacja pochodzi z serwisu: wiadomosci.tvp.com.pl – z dn.03.10.2000r.

miękkich narkotyków. Ich sprzedaż nie jest zabroniona np. w Holandii (oczywiście dopuszczalna jest pod pewnymi warunkami). Przepisy umożliwiające też proceder są jak widać skrupulatnie wykorzystywane. Handel narkotykami, środkami psychotropowymi i bronią stanowią nie lada wyzwanie dla legislatorów. Wskazać należy, że bez wspólnych, jednakowych przepisów nie będzie możliwe skuteczne zwalczanie tych zjawisk w sieci.

Czyny opisane w art. 255, 256 i 257 k.k. są kolejnymi odmianami przestępstw. Nie podlega dyskusji kwestia publiczności Internetu. Dziś to medium jest traktowane na równi z telewizją i radiem, więc wszelkie zamieszczane w nim treści powinny odpowiadać prawu na równi z innymi środkami przekazu.

Ciekawym zjawiskiem jest e-terrorizm. Ostatnie wydarzenia na Bliskim Wschodzie pokazują, że przyszłe konflikty mogą przenosić się do cyberprzestrzeni. Niszczenie stron przeciwnika, blokowanie, a wręcz destabilizacja, systemu (czy to dowodzenia czy informacji) mogą spowodować czasami większe szkody od tych wyrządzanych środkami tradycyjnymi. Inteligentna broń na polu walki to broń XXI wieku. Wszystko to sprawie, że zarówno wojna jak i terrorizm mogą przybrać nowe oblicze.

Rozwój Internetu nie uszedł uwagi służbom wywiadowczym. Znalazło to także odbicie w nowym k.k. (art. 130 §3). Pozyskiwanie informacji dzięki sieci jest łatwe i tanie. Trwa nieustanny wyścig pomiędzy *hackerami*, a firmami produkującymi zabezpieczenia. Dziś wiemy, że nie ma doskonałego zabezpieczenia. Istnieje tylko kwestia czasu, który trzeba poświęcić na jego złamanie.

Skoro można się porozumiewać poprzez sieć, można także zniesławiać i znieważać. Odpowiednie zastosowanie znajdują więc art. 216 §2 i 212 §2 k.k. jako, że Internet jest środkiem masowego komunikowania się. Do tej pory niewiele spraw trafiło na wokandę, jednak zauważyć można dużą dynamikę tego typu przestępstw. Ścigane są one z oskarżenia prywatnego i będą w coraz większym stopniu dotyczyły Internetu, gdyż zapewnia on dużo większą swobodę publikacji niż np. radio, prasa czy telewizja. Do naruszania dóbr osobistych w sieci jeszcze powrócę przy omawianiu prawa cywilnego.

Cyberprzestrzeń i szeroko rozumiane sieci komputerowe stanowią doskonale narzędzie przestępstwa. Dziś nawet sobie nie wyobrażamy skali zjawiska i trudno objąć wszelkie możliwości, które daje „klawiatura czy myszka”.

Oto trochę przykładów:

- elektroniczne zabójstwo, art. 148 k.k. - poprzez odłączenie od aparatury podtrzymującej życie, zmianę proporcji lekarstwa- wszystko to możliwe jest dzięki sieci<sup>101</sup>;

- bezczeszczenie symboli narodowych, art. 137 k.k. - ponieważ dotyczy to przede wszystkim nie samych przedmiotów materialnych lecz uczuć osób żywiących szacunek do tych symboli;

- spowodowanie katastrofy, art. 163 k.k. - ingerencja w sieć komputerową elektrowni atomowej czy wyłączenie systemu przeciwpożarowego;

- spowodowanie katastrofy w komunikacji, art. 173 k.k.- poprzez przejęcie kontroli nad samolotem czy pociągiem i doprowadzenie do wypadku;

---

<sup>101</sup> K.J. Jakubski, *Przestępczość komputerowa- próba zdefiniowania zjawiska*, [w:] R. Skubisz (red), *Internet-problemy prawne*, op. cit., s. 268.

- znaczne zniszczenie środowiska, art. 181 k.k.- przejęcie kontroli nad systemem oczyszczalni ścieków;
- groźba karalna, art. 190 k.k.;
- rozpowszechnianie wiadomości z postępowania przygotowawczego, art. 241 §1 k.k.;
- ujawnianie tajemnicy państwowej i służbowej art.265 i 266 k.k.;
- wpływanie na wynik głosowania, art. 248 k.k.- co prawda dziś się to jeszcze nie zdarza lecz tylko dlatego, że nie mamy wyborów *on-line*;
- fałszowanie dokumentów, art. 270 k.k.- pojawiły się dokumenty w formie elektronicznej i prawdopodobnie nie pozostanie to bez odzewu ze strony środowiska fałszerzy – informatyków;
- pranie brudnych pieniędzy, art. 299 k.k.

Przykładów, które ilustrują przestępcze wykorzystywanie sieci jest dużo. Obrazuje to tylko skalę e-przestępczości. Problem jednak polega na tym, że bez przyjęcia ogólnościowych standardów i zabezpieczeń trudno będzie powstrzymać czy też choć ograniczyć działalność elektronicznych przestępców.

### 3. Prawo karne procesowe

#### Zagadnienia wstępne

Potrzeba uwzględnienia przez przepisy procedury karnej obecności nowych technik przetwarzania informacji w życiu społecznym wynika z dwóch okoliczności. Po pierwsze z typizacji przez prawo karne materialne tzw. przestępstw komputerowych, konieczności stworzenia proceduralnych podstaw ich ścigania. Po drugie – i jest to powód co najmniej równie istotny- z faktu, że system komputerowy czy telekomunikacyjny może być wykorzystywany do popełniania przestępstw tradycyjnych i zawierać ich dowody<sup>102</sup>.

Już na samym wstępie pojawia się ważna kwestia jurysdykcji krajowej. Co prawda reguluje ją art. 5 k.k. lecz zajmę się nią w tej części pracy. Kodeks określa do jakich podmiotów stosuje się polską ustawę karną. Zwróćmy jednak uwagę, że określenia „terytorium Rzeczypospolitej Polskiej” nie można przenieść na grunt cyberprzestrzeni. Nie posiada ona jednak granic. Problem z ustaleniem miejsca i czasu popełnienia przestępstwa zasygnalizowałem w podrozdziale dotyczącym prawa karnego materialnego. Z miejscem zdarzenia wiąże się właściwość miejscowa sądów powszechnych.

Skoro trudno będzie określić miejsce popełnienia przestępstwa zaistnieją także przeszkody w ustaleniu właściwości miejscowej. I choć tę kwestię rozwiązuje §3 art.31 k.p.k. to może zdarzyć się taki przypadek, że mimo dokonania czynu zabronionego żaden sąd nie rozpatrzy danej sprawy. Innym utrudnieniem ścigania przestępstw komputerowych (elektronicznych) może być często stosowana klauzula niskiej szkodliwości społecznej czynu. Zawarta jest ona w §2 art. 2 k.k., w art. 17 §1 pkt 3 k.p.k., a sama definicja pojęcia wyrażona została w artykule 115 §2 k.k.. Mały stopień wiedzy o przestępstwach komputerowych, skali wyrządzanych

<sup>102</sup> A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 181.

przez nie szkód oraz wciąż duży odsetek nieujawnionych nadużyć komputerowych sprawiają, że często owe czyny mogą być przez wymiar sprawiedliwości niedoceniane<sup>103</sup>.

## Czynności procesowe

W przypadku związku Internetu z postępowaniem karnym należy zwrócić uwagę na kwestię czynności procesowych (dział IV k.p.k.).

Znaczącą rolę odgrywa w procesie karnym czynność doręczenia. Kodeks określa listę podmiotów, które dokonują doręczeń. I tak są to: poczta, funkcjonariusz organu wysyłającego, policja (w razie konieczności), oraz na mocy art. 134 k.p.k. przełożeni żołnierzy, funkcjonariuszy Policji, UOP, Straży Granicznej i Służby Więziennej, a osobom pozbawionym wolności administracja odpowiedniego zakładu. Artykuł 131 §2 k.p.k. określa specyficzny przypadek. Dopuszcza się jednocześnie zawiadomienia poprzez ogłoszenie w prasie, radiu lub telewizji. Poruszyłem już na samym wstępie pracy kwestię zakwalifikowania Internetu do prasy. Czy więc k.p.k. dopuszcza zawiadamianie w trybie art. 131 §2 na łamach prasy internetowej?

Należy odpowiedzieć na to pytanie twierdząco zważywszy, iż ustawodawca wyszedł tu z założenia, że liczy się dotarcie do „tyłu pokrzywdzonych, że ich indywidualne zawiadomienie o przysługujących im prawach spowodowałoby poważne utrudnienia w prowadzeniu postępowania”. Internet pozwala na szybkie i bezpośrednie dotarcie tak do indywidualnego użytkownika jak i nieokreślonej grupy osób. Jest więc w tym przypadku bardzo pomocnym narzędziem do zawiadamiania danych osób. Z punktu widzenia zastosowania Internetu w procesie karnym art. 137 odgrywa niebagatelną rolę. Pozwolę sobie przytoczyć jego treść: *W przypadkach nie cierpiących zwłoki można wzywać lub zawiadamiać osoby telefonicznie albo w inny sposób stosownie do okoliczności, pozostawiając w aktach odpis nadanego komunikatu z podpisem osoby nadającej.*

„Innym sposobem” oprócz wezwania, czy zawiadomienia telefonicznego, określonego w tym artykule będzie np. faks, teleks, Internet<sup>104</sup>. Same orzecznictwo także wypowiedziało się w tej kwestii: *Adres do doręczeń pisemnych, numer telefonu czy adres elektroniczny dla zawiadomień w tych formach są ofertą dla sądu, by korzystał z każdej z tych form przekazywania wiadomości*<sup>105</sup>.

W przepisie tym (art. 137 k.p.k.) wskazano tylko jeden sposób przekazywania informacji- telefonicznie- z jednoczesnym ogólnym wskazaniem, że może to nastąpić w inny sposób. Oznacza to każdy technicznie dostępny doręczającemu i adresatowi sposób komunikowania się, zapewniający przekazanie wezwania lub zawiadomienia, a więc np. telegraf, fax, pocztę elektroniczną. Musi być przy tym spełniony warunek, że adresat, w tym wypadku faxu, poczty elektronicznej posługuje się urządzeniami tego rodzaju, o czym poinformował

<sup>103</sup> W Polsce w styczniu 2000 r. prowadzonych było 22 dochodzenia w sprawie przestępstw internetowych- 10- dotyczyło rozpowszechniania treści pornograficznych, rasistowskich i obrażających grupy wyznaniowe, 7 – handlu pirackimi programami komputerowymi i fonograficznymi, 5- korzystania w sklepach internetowych ze skradzionych kart płatniczych lub ich komputerowo wygenerowanych numerów. R. Kamiński, *Internet poza prawem*, „Wprost” z 20.01.2000.

<sup>104</sup> J. Satko glosa OSP 199/3/66 do postanowienia SN z dn. 20.10.1998, III Kz 182/98.

<sup>105</sup> Postanowienie sądu apelacyjnego z 20.01.1999r.III Akz 13/99, KZS 1999/2/27 w Krakowie.

organ doręczający albo wszystkich zainteresowanych np. przez zgodę na publikację takiej informacji w informatorze okręgowej rady adwokackiej<sup>106</sup>. Pozostawienie w aktach odpisu nadanego komunikatu z podpisem osoby nadającej w przypadku przesłania wiadomości pocztą elektroniczną nastąpi w formie notatki urzędowej.

Może na przestrzeni kilku lat, w ramach coraz powszechniejszego dostępu do sieci ta właśnie forma zawiadamiania wyprze pozostałe. Lecz na razie pozostaje nam zwykła biała koperta wraz z zawartością.

## Dowody

Dowód w postępowaniu karnym to każdy dopuszczalny przez prawo karne procesowe środek, służący dokonaniu takich ustaleń czyli służący ustaleniu okoliczności mających znaczenie dla rozstrzygnięcia<sup>107</sup>. Zobaczmy więc czy postępowanie karne dopuszcza dowód z Internetu i jaki jest jego wpływ na sam proces dowodzenia.

Informacje- dane- zawarte w pamięci komputera nie są rzeczą. Jednak w stosunku do samego komputera (nośnika informacji) będzie można zastosować przepisy k.p.k. o oględzinach rzeczy (art. 207 mówi o oględzinach miejsca, rzeczy, osoby). Rzeczą jest także dokument, jeśli badamy nie jego treść intelektualną lecz cechy fizyczne (autentyczność, autorstwo). Paragraf 2 art. 207 k.p.k. ma duże znaczenie w przypadku informacji i elektronicznych dokumentów. Nietrwałość zapisu oraz jego łatwość zniszczenia (z zewnątrz czy też przez osoby badające komputer) pozwala na zastosowanie owego przepisu. Utrwalenie, o którym jest mowa będzie następowało poprzez zapisanie na elektronicznym nośniku danych (najlepszym rozwiązaniem jest zapis na niemodyfikowalnych dyskach optycznych typu WORM).

Pamiętajmy także o dokumencie (czyli każdym przedmiocie lub zapisie na komputerowym nośniku informatycznym (...) -art. 115 §14 k.k.), który jako rzecz będzie podlegał oględzinom. W Internecie możemy wyróżnić dokumenty urzędowe i prywatne. Nie można jednak dzielić ich na pierwotne i pochodne, gdyż kopia oryginalnego dokumentu ma takie same cechy fizyczne jak pierwowzór (po dokonaniu modyfikacji w programie ustalającym datę wykonania kopii).

Kodeks dopuszcza przeprowadzenie eksperymentu procesowego (art. 211 k.p.k.) . Można go rozumieć dwojako. Pierwsze jako doświadczenie- polega na sprawdzeniu możliwości wystąpienia określonych faktów lub zjawisk bądź zbadania możliwości ich spostrzeżenia w danych warunkach<sup>108</sup>. Drugie- to odtworzenie warunków oraz sprawdzenie czy dane zdarzenie mogło w dany sposób przebiegać. Oba te przypadki odnoszą się także do Internetu. Komputer podłączony do sieci może być doskonałym źródłem dowodowym, ukazującym określone działanie w cyberprzestrzeni.

Ciekawym zagadnieniem procesowym w ujęciu elektronicznym jest zatrzymanie rzeczy i przeszukanie. Podkreślić należy, że obie te instytucje są jawne. Odróżniają się tym właśnie od elektronicznego podsłuchu. Zatrzymanie

---

<sup>106</sup> J. Grajewski, L.K. Peprzycki, *Kodeks Postępowania Karnego z komentarzem*, Sopot 2000 , s. 214.

<sup>107</sup> T.Grzegorzczak, J. Tylman, *Polskie postępowanie karne*, Warszawa 1999, s. 414.

<sup>108</sup> Ibidem, s. 479.

rzeczy obejmuje m.in. rzeczy mogące stanowić dowód w sprawie (217 §1k.p.k. *in principio*) w tym także korespondencję i przesyłki mające znaczenie dla postępowania, a znajdujące się w dyspozycji urzędów, instytucji i podmiotów prowadzących usługi poczty i telekomunikacji, urzędów celnych oraz instytucji i przedsiębiorstw transportowych (art. 218 §1 k.p.k.) . Wydaniu rzeczy może podlegać sam dokument jak i nośnik informacji, na którym jest on zapisany (czyli komputer). O ile wydanie dokumentu elektronicznego (w formie kopii) nie może być uciążliwe tak wydanie sprzętu komputerowego może taką okoliczność stanowić. Wkracza tu jednak wskazana w art. 227 k.p.k. zasada proporcjonalności. Zatrzymanie wielu urządzeń technicznych, gdy doprowadzałoby to do unieruchomienia przedsiębiorstwa lub dużych strat powinno być stosowane rzadko i tylko w uzasadnionych przypadkach.<sup>109</sup>

Przeszukanie zostało uregulowane w art. 219 k.p.k. i następnych 220-224. Wprawdzie mowa tam o przeszukaniu „pomieszczeń lub innych miejsc” lecz możemy przepis ten zastosować także wobec sieci. Należy jednak odróżnić samą czynność przeszukania od tzw. przeglądania (inaczej zwanego patrolowaniem). W ramach swych ustawowych uprawnień (art. 14 i 20 ustawy o Policji) funkcjonariusze mogą wykorzystywać do celów związanych z rozpoznawaniem i zapobieganiem przestępstwom zarówno informacje rozpowszechniane w Internecie – np. przez serwery WWW czy grupy *Usenet*, a także brać udział w charakterze obserwatorów lub aktywnych uczestników we wszelkich otwartych forach wymiany informacji i komunikowania się w rodzaju list dyskusyjnych lub kanałów IRC<sup>110</sup>.

Przy przeszukaniu komputera, zabezpieczonego hasłem pojawia się kwestia czy organy ścigania mają owo hasło złamać czy też uzyskać je od podejrzanego (oskarżonego). W tym drugim przypadku nie możemy przyjąć aby sam podejrzany dostarczał dowodów na swoją niekorzyść (art. 75 §1 k.p.k.). Nie ma więc on obowiązku udostępniania hasła broniącego dostępu do jego urządzenia technicznego. Odmiennie przedstawia się w tym zakresie sytuacja prawna innych podmiotów, które mają obowiązek aktywnego współdziałania z organami prowadzącymi postępowanie karne (...) <sup>111</sup>. Uwagę zwraca zagrożenie związane z przeszukiwaniem zbiorów danych przez organy ścigania, gdyż może to prowadzić do ograniczenia swobód obywatelskich i inwigilacji obywateli.<sup>112</sup>

## Podśluch telekomunikacyjny i elektroniczny

Art. 237 k.p.k. określa podśluch telekomunikacyjny- jest to uzyskiwanie dowodów przestępstwa na podstawie kontroli i utrwalania rozmów telefonicznych. Jednak na podstawie art. 241 przepisy z rozdziału 26 k.p.k. (kontrola i utrwalanie rozmów) stosuje się odpowiednio do kontroli oraz

---

<sup>109</sup> Wspomnieć tu należy, iż sam fakt przejęcia systemu przez policję może być przyczyną do nie zawiadomiania organów ścigania przez poszkodowanego o przestępstwie- A. Adamski, *Prawo karne komputerowe*, op. cit., s. 19.

<sup>110</sup> A. Adamski, *Prawo karne komputerowe*, op. cit., s. 210.

<sup>111</sup> Ibidem. s.214.

<sup>112</sup> Por. U Sieber: *The International Emergence of Criminal*, s.49. oraz *Information Law*, Koln- Berlin-Munchen, 1992, s.13.

utrwalania, przy użyciu środków technicznych treści przekazów informacji innych niż rozmowy telefoniczne.

Tak więc przepisy te stosuje się do Internetu i podsłuchu elektronicznego (przede wszystkim poczty elektronicznej, IRC, ICQ i innych technik w ramach sieci). Nie zmienia to faktu, że informacje uzyskiwane i rejestrowane są w czasie rzeczywistym czyli podczas przesyłania siecią telekomunikacyjną<sup>113</sup>.

Nie spełnia przesłanek z art. 237 k.p.k. „zwykły” podsłuch bezpośredni- np. przy pomocy ukrytych mikrofonów. Sam przepis art. 241 k.p.k. jest ustawowym wyjątkiem od konstytucyjnej zasady ochrony komunikowania się. Dotyczy on tylko treści przekazów informacji w telekomunikacji. Owo ograniczenie wolności obywatelskiej może nastąpić jedynie na podstawie decyzji sądu na wniosek prokuratora, a w wypadkach nie cierpiących zwłoki może zarządzić je sam prokurator (art. 237 §1 i 2 k.p.k.). Poza tym kontrola i utrwalanie rozmów i informacji przesyłanych siecią telekomunikacyjną są dopuszczalne tylko gdy toczące się postępowanie lub uzasadniona obawa popełnienia nowego przestępstwa dotyczy czynów zabronionych, wymienionych taksatywnie w §3 art. 237 k.p.k.

Duża liczba – 16 – przestępstw objętych przepisem oraz konstrukcja §4, w którym w zakres osób, objętych potencjalnym podsłuchem zaliczono osobę, która może mieć związek ze sprawcą lub grożącym przestępstwem, powodują, że swoboda komunikacji może być w łatwy sposób łamana. I choć piśmiennictwo wyklucza z grona zagrożonych podsłuchem osoby objęte immunitetem<sup>114</sup> to instytucja ta może bezpośrednio zagrażać podstawom demokratycznego państwa prawa.

Polski k.p.k. ustanawia zasadę jawności rozprawy. Ograniczenie jawności określone zostało w art. 355 ustawy. Jaki związek ma jawność rozprawy z Internetem? Otóż na podstawie art. 357 k.k. (udział mediów) możemy stwierdzić, że przedstawiciele radia, telewizji i prasy (wszystkie trzy środki masowego przekazu mają także swe odpowiedniki w sieci) mogą dokonywać utrważeń dźwięku i obrazu. Czy zatem w świetle tego przepisu możemy spodziewać się relacji „na żywo” z rozprawy w Internecie?

Należy na to pytanie odpowiedzieć twierdząco. Po spełnieniu warunków określonych w art. 357 §1 i 2 k.p.k. jest to dopuszczalne. A zatem sprawy karne w Internecie? Tak i to już niedługo (należy wspomnieć np. o elektronicznych operacjach lekarskich i o e-konferencjach). Takie rozwiązanie realizowałoby w pełni zasadę udziału czynnika społecznego w postępowaniu karnym oraz wpływało dodatnio na niezawisłość sędziów.

Ciekawym problemem jest kwestia komunikacji. Tak świadków ze sobą jak i (podejrzanego) oskarżonego z obrońcą. Przewodniczący powinien przedsięwziąć środki zapobiegające porozumiewaniu się osób przesłuchiowanych z osobami, które jeszcze nie zostały przesłuchane – art. 371 §2 k.p.k.. W dobie uniwersalizacji i minimalizacji urządzeń telekomunikacyjnych Internet może prowadzić do obchodzenia zakazów i utrudniania postępowania.<sup>115</sup>

---

<sup>113</sup> Nie spełnia tych przesłanek utrwalanie przekazu zanim znalazł się on w sieci telekomunikacyjnej lub ją opuścił w postaci „fal głosowych”.

<sup>114</sup> B. Kurzepa, *Kontrola i utrwalanie rozmów telefonicznych wg k.p.k.*, Prok. i Pr. 1999/3/77.

<sup>115</sup> Rozwiązanie leży tu w środkach czysto technicznych np. pozostawianie wszelkiego sprzętu elektronicznego w depozycie przed wejściem do budynku sądu.

Art. 73 reguluje porozumiewanie się podejrzanego z obrońcą. Nie tylko połączenie telefoniczne ale i Internet mogą zmierzać do omijania zastrzeżeń przewidzianych w §2 art. 73 k.p.k.

Omówione przeze mnie instytucje prawa karnego materialnego i procesowego pokazują, że ustawodawca dostrzega zachodzące zmiany i próbuje nadrobić stracony czas. Potrzeba jednak jeszcze wielu zmian, aby polskie prawo karne było przygotowane na dalszy rozwój sieci. Konieczne są rozwiązania sięgające w przyszłość, przepisy, które po roku obowiązywania nie staną się martwe. Potrzeba do tego dużej wiedzy, stałego monitorowania środowiska a także, przede wszystkim, dalekowzroczności i wyobraźni jeśli chodzi o wszystko co wiąże się z Internetem.

## 4.Prawo prasowe

### Internet a prasa

Kolejną gałęzią prawa publicznego, która wykazuje silne związki z Internetem jest prawo prasowe. Tu pojawiają się dwa zasadnicze pytania:

Czy Internet jest prasą? oraz jak oceniać prasę w Internecie? Jednak problemów dotyczących związku sieci z prawem prasowym jest znacznie więcej. Przyglądnijmy się więc tym najbardziej doniosłym.

„Rzeczpospolita Polska zapewnia wolność prasy i innych środków społecznego przekazu”. Przytoczony art.14 Konstytucji RP odnosi się do szeroko rozumianej prasy. Definicję tego pojęcia znajdujemy w ustawie prawo prasowe z dnia 26.01.1984 r.(Dz.U.84.5.24).

Przepis art.7 ust.2 pkt.1 tejże ustawy stanowi: *Prasa oznacza publikacje periodyczne, które nie tworzą zamkniętej, jednorodnej całości, ukazujące się nie rzadziej niż raz do roku, opatrzone stałym tytułem albo nazwą, numerem bieżącym albo datą, a w szczególności: dzienniki i czasopisma, serwisy agencyjne, stałe przekazy teleksowe, biuletyny, programy radiowe i telewizyjne oraz kroniki filmowe; prasą są także wszelkie istniejące i powstające w wyniku postępu technicznego środki masowego przekazywania, w tym także rozgłoszenie oraz tele - i radiowęzły zakładowe upowszechniające publikacje periodyczne za pomocą druku, wizji, fonii lub innej techniki rozpowszechniania; (...)*.

Na gruncie owego przepisu należy stwierdzić, że nie możemy stosować ustawy do całego Internetu, który zapewnia komunikację nie tylko masową (elektroniczne wydania gazet) lecz także grupową (grupy dyskusyjne) oraz indywidualną (poczta elektroniczna). Jednak sama definicja jak i jej zastosowanie do Internetu budzi wiele zastrzeżeń i kontrowersji. Samo ukazanie się (choć i periodyczne) materiału w sieci nie powoduje już uznania go za prasę wraz ze wszelkimi tego konsekwencjami. Takie zaprezentowanie odbywa się na zupełnie innych zasadach niż w tradycyjnej prasie. Publikacja w sieci jest często anonimowa, nie poprzedza jej nadzór redakcyjny, ocena i sprawdzenie materiału ze strony uprawnionych do tego osób, dokonuje się bez rejestracji, która dotyczy zwykłej prasy.

Jeśliby jednak uznać, iż Internet „jako taki” objęty jest podaną wyżej szeroką i dość elastyczną definicją prasy, to pojawiłoby się zaraz następne pytanie: czy

mając na uwadze, iż informacje są tu rozsyłane drogą fal elektromagnetycznych powinno się go raczej traktować podobnie jak radio i telewizję, czy też bardziej właściwe byłoby dopatrywanie się podobieństw z prasą drukowaną.<sup>116</sup> Uregulowania dotyczące owych dwóch grup mediów różnią się w znaczący sposób co powoduje, że ów problem ma doniosły charakter.

Gdyby uznać cały Internet za prasę doprowadziłoby to, na gruncie prawa autorskiego, do odpłatnego rozpowszechniania (bez zgody odpowiedniego podmiotu) w celach informacyjnych różnych materiałów, między innymi wcześniej już rozpowszechnionych, aktualnych artykułów oraz wypowiedzi na tematy polityczne, gospodarcze i społeczne. Nieodpłatnie zamieszczano by natomiast: krótkie streszczenia utworów tzw. przegląd prasy, mowy wygłoszone na publicznych zebraniach i rozprawach, rozpowszechnione sprawozdania o aktualnych wydarzeniach. Swobodne byłoby dalsze publikowanie w Internecie aktualnych zdjęć reporterskich (odpłatnie).

W przypadku innych aktów prawnych należy zastanowić się czy Internet jest „środkiem masowego przekazu”. Problem ten na gruncie prawa karnego omówiłem w poprzednim rozdziale, lecz dotyczy on także reklamowania leków wydawanych wyłącznie z przepisu lekarza<sup>117</sup>.

Informacje podawane przez sieć są- w rozumieniu prawa- „informacjami podawanymi do publicznej wiadomości”. Takie stanowisko wywołuje konsekwencje w obszarze tych regulacji, które posługują się tak właśnie sformułowaną przesłanką (na przykład w sferze dotyczącej informacji na temat sprzedaży papierów wartościowych)<sup>118</sup>.

## Reklama w sieci

Innym ciekawym zagadnieniem jest reklama w sieci. Internet to doskonałe medium reklamowe. Lepsze od radia, drukowanej prasy a nawet telewizji. Przewagę taką dają mu trzy możliwości techniczne związane z jego działaniem:

- zasięg (globalny – jak żadnego innego medium- oraz stale zwiększająca się ilość użytkowników),
- niskie koszty (dużo taniej jest zaprezentować reklamę w sieci niż stworzyć takową w telewizji),
- trwałość (reklama nie znika i nie trwa tak krótko jak w telewizji czy radiu).

Dodatkową zaletą jest swoiste przerzucenie kosztów samej reklamy na klienta. To przecież on może ją wydrukować czy zapisać. Licznik zamieszczony na stronie WWW pozwala zorientować się ile osób daną reklamą się zainteresowało. Dzięki językowi Java możliwe jest kierowanie konkretnej reklamy do indywidualnych odbiorców (*Advertising on demand, real time marketing*). Poszczególne protokoły wskazują jaki był czas wyświetlanej reklamy, stopień zainteresowania oraz tzw. sukces reklamowy- gdyż dzięki elektronicznym ofertom można towar zakupić bezpośrednio w sieci. Internet daje także możliwość

---

<sup>116</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.35.

<sup>117</sup> Art.4 ust.2 ustawy z dn.10 października 1991 r. o środkach farmaceutycznych, materiałach medycznych, aptekach, hurtowniach i nadzorze farmaceutycznym (Dz.U. nr 105, poz.452 z późn. zmianami).

<sup>118</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit, s.38.

budowania bazy danych o klientach oraz osobach zainteresowanych danym produktem. Same bazy danych są już dziś swoistym towarem.

W Internecie można wyróżnić następujące rodzaje reklamy:

- *Bannery* – to forma graficzna (statyczna lub animowana), kliknięcie powoduje przeniesienie internauty do serwisu reklamodawcy;
- *Mailing* – wysyłanie *e-maili* z tekstem promocyjnym do właścicieli kont poczty elektronicznej;
- *Sponsoring* – częściowe finansowanie witryny w zamian za umieszczenie logo lub innych elementów według życzeń sponsora;
- Wykupywanie słów kluczowych w wyszukiwarkach internetowych;
- *Interstitials* – wypełnianie całego okna przeglądarki treścią reklamową w chwili ładowania kolejnej strony serwisu;
- *Pop up windows* – w chwili przejścia z jednej strony serwisu na drugą następuje otwarcie nowego, małego okna z treścią reklamową<sup>119</sup>.

Definicja reklamy zawarta w art. 4 pkt.6 ustawy o radiofonii i telewizji z dn. 29.12.1992 r. (Dz. U. z 1993 r. nr 7, poz.34, z późn. zmianami) określa ją jako każdy przekaz zmierzający do promocji sprzedaży albo innych form korzystania z towarów lub usług, popieranie określonych spraw lub idei albo do osiągnięcia innego pożądanego przez reklamodawcę celu nadawany za opłatą lub inną formę wynagrodzenia. Na gruncie owej definicji pojawiają się swoiste problemy. Z uwagi jednak na ramy mojego opracowania zmuszony jestem je pominąć.

Kwestia reklamy uregulowana jest przede wszystkim w art. 36 ustawy prawo prasowe oraz w przepisach prawa podatkowego, dotyczących podatku dochodowego od osób fizycznych<sup>120</sup> oraz podatku dochodowego od osób prawnych<sup>121</sup>. Problem nieuczciwej reklamy został unormowany w ustawie z dn. 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji<sup>122</sup> (Dz.U.93.47.211.).

## Prasa w Internecie i jej cenzura

Przejdźmy teraz do kolejnego zagadnienia, a mianowicie prasy w Internecie. Dziś niemal wszystkie dzienniki i czasopisma znajdują swe odpowiedniki w sieci. Występuje także e-prasa, która nie ma swego odpowiednika w zwykłej formie. Wydawcy poszerzają swą ofertę poprzez udostępnianie swych produktów w formie elektronicznej. Jaki jest więc status prawny owych elektronicznych publikacji w Internecie?

Wiąże się z tym szereg problemów. Jednym z nich jest kwestia sprostowania informacji zamieszczonej w obu wydaniach (zwykłym i elektronicznym) gazety. Czy poszkodowanemu podmiotowi przysługuje roszczenie o sprostowanie informacji nie tylko na łamach drukowanej prasy lecz także w elektronicznym wydaniu? Gdzie szukać podstawy prawnej takiego roszczenia skoro przepisy o sprostowaniu nie stanowią o ich umieszczeniu w Internecie?

---

<sup>119</sup> ZUM, *Niebanalne bannery*, „Gazeta Wyborcza” z dn. 30.10.2000 r.

<sup>120</sup> Patrz art.23 ust.1 pkt.23 ustawy z dn. 26.07.1991 r.

<sup>121</sup> Patrz art.16 ust.1 pkt. 28 ustawy z dn. 15.02.1992 r.

<sup>122</sup> Patrz szerzej: E. Nowińska *Nieuczciwa reklama w internecie- problemy prawne* [w:] R. Skubisz,, *Internet – problemy prawne*, op. cit., s.51-64.

Zbliżone dylematy powstawać mogą odnośnie ogłoszenia odpowiedzi, a także komunikatów urzędowych, prawomocnych wyroków lub innych orzeczeń zawierających klauzulę o opublikowaniu, ogłoszeń sądu lub innego organu państwowego. Przepisy nakładają w tej mierze na prasę określone obowiązki.<sup>123</sup> Należy przyjąć jednak stanowisko, iż zamieszczenie sprostowania, odpowiedzi, orzeczenia, ogłoszenia, komunikatu powinno występować we wszystkich rodzajach prasy. W zajęciu odmiennego stanowiska można by upatrywać naruszenia słuszných interesów zarówno tego, komu przysługuje uprawnienie do domagania się opublikowania materiału jak i czytelników<sup>124</sup>.

Ciekawym problemem jest także rejestracja elektronicznej prasy. W przypadku uznania takich publikacji za prasę mają zastosowanie przepisy ustawy o prawie prasowym (art. 20-23a) o rejestracji dziennika lub czasopisma. Czy podlegają temu obowiązkowi elektroniczne edycje prasy drukowanej czy też tylko te, nie mające swych odpowiedników na rynku „zwykłej prasy”? Czy też może obowiązkiem rejestracji objąć wszystkie ukazujące się w Internecie dzienniki i czasopisma?

Tu właśnie daje się zauważyć różnice, które charakteryzują elektroniczne wydania prasy. Czy rozpatrywać taką formę jako dalszy powszechnie udostępniony „egzemplarz” danego tego samego periodyku, czy też w istocie już jako inny periodyk względnie jako swego rodzaju „mutację” pisma podstawowego<sup>125</sup>. W przypadku elektronicznej formy czytelnik uzyskuje szereg możliwości niedostępnych w tradycyjnych wersjach. Mowa tu o: tak zwanych linkach i hiperlinkach, poprzez które można dotrzeć do dodatkowych informacji, zdjęć, wyrażaniu swych opinii poprzez fora dyskusyjne, udostępnianiu ankiet oraz innych specyficznych informacjach (dostępność przekazu audio i video).

W przypadku zaliczenia elektronicznych periodyków do prasy zastosowanie miałyby do nich przepisy dotyczące udostępniania im przez organy państwowe, przedsiębiorstwa państwowe i inne państwowe jednostki organizacyjne, a w zakresie działalności społeczno-gospodarczej również organy spółdzielcze i osoby prowadzące działalność gospodarczą informacji o swojej działalności<sup>126</sup>.

Wszystkie przedstawione zagadnienia dotyczą także funkcjonowania radia i telewizji w sieci. Internet wpływa na ich działalność, niejednokrotnie zmieniając ich oblicze. Pojawia się coraz więcej programów, w których nie pośrednią rolę odgrywa sieć. Stacje radiowe prezentują w cyberprzestrzeni zdjęcia ze studiów, nagrania poszczególnych audycji, program nadawania oraz wiele innych informacji. Telewizja zagrożona przez Internet coraz częściej korzysta dziś z nowego medium. Już w niedalekiej przyszłości powszechne stanie się przeglądanie stron na ekranie telewizora<sup>127</sup>. Same stacje telewizyjne prowadzą już aktywną politykę w kierunku cyfrowego i elektronicznego rozwoju.

Osobnym zagadnieniem jest cenzura prasy. Ustęp 2 artykułu 54 Konstytucji RP stwierdza, że cenzura prewencyjna środków masowego przekazu oraz

<sup>123</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 42.

<sup>124</sup> Ibidem, s.43.

<sup>125</sup> Ibidem, s.43.

<sup>126</sup> Art. 4 ustawy prawo prasowe z dn. 07.02.1984 r.

<sup>127</sup> V. Makarenko, *TV Internet*, „Gazeta Wyborcza” z 27.12.2000 r. oraz V. Makarenko *Najpierw Kraków i Warszawa*, wywiad z E. Kurek.

koncesjonowanie prasy są zakazane. Jednak pojawiają się coraz to nowe inicjatywy dotyczące cenzury Internetu.<sup>128</sup> W przypadku naruszenia prawa nie będziemy mieli do czynienia z cenzurą lecz z przestępstwem <sup>129</sup>, a przy takowym organa ścigania i sądy wyposażone są w odpowiednie instrumenty prawne.

Podsumowując rozważania na temat prasy w Internecie i prawa prasowego należy zwrócić uwagę na wiele niewyjaśnionych problemów wiążących się z tą tematyką. Odpowiedź na nasuwające się pytania przyniesie czas. Już dziś należy stwierdzić, że konieczne są bardziej precyzyjne przepisy dotyczące bezpośrednio działalności szeroko rozumianej prasy w cyberprzestrzeni oraz funkcjonowania samego Internetu.

## 4. Prawo finansowe

Prawo finansowe to kolejna gałąź prawa publicznego, z którą ściśle związany jest Internet. Także tu, tak jak w poprzednich dziedzinach prawa, możemy zauważyć rosnące znaczenie sieci. Informatyzacja i komputeryzacja zmieniają oblicze finansów.

Nauka przyjmuje różną systematykę prawa finansowego dla potrzeb jednak tej pracy przytoczę jedną z koncepcji za Aliną Majchrzycką-Guzowską<sup>130</sup>. Systematyka prawa finansowego kształtuje się następująco:

- prawo budżetowe,
- prawo podatkowe,
- prawo celne,
- prawo finansowe ubezpieczeń państwowych,
- prawo finansowe samorządu terytorialnego,
- prawo walutowe i dewizowe,
- prawo bankowe,
- prawo finansowe podmiotów gospodarczych.

Coraz więcej transakcji zawieranych jest poprzez Internet. Możemy je podzielić na bezpośrednie (to te, w których następuje przekazanie usługi czy towaru za pomocą sieci- czyli przede wszystkim dotyczy to produktów cyfrowych- fotografii, programów komputerowych, baz danych, nagrań muzycznych oraz usług takich jak konsultacje, porad, obsługi sieciowej, poczty elektronicznej, reklamy) oraz pośrednie. W tych ostatnich dostawa towaru następuje m.in.. za pomocą poczty czyli poprzez fizyczne dostarczenie przedmiotu transakcji.

Z uwagi na złożoność problemu i jego rozmiary skoncentruję się, przede wszystkim, na dwóch dziedzinach prawa finansowego, a mianowicie na prawie podatkowym i prawie bankowym.

---

<sup>128</sup> Projekt rozporządzenia MSWiA dostępny także na [www.vagla.eu.org/projekt\\_mswia.htm](http://www.vagla.eu.org/projekt_mswia.htm). Zob. też M. Rybarczyk, *Tu Wielki Brat*, „Gazeta Wyborcza” z 04.12.2000 r.

<sup>129</sup> B. Mikołajewska, *Sieć na sieć*, „Polityka” z dn. 28.10.2000 r.

<sup>130</sup> A.Majchrzycka-Guzowska, *Finanse i prawo finansowe*, Warszawa 1998, s 17.

## Prawo podatkowe

Zwiększający się handel towarami i usługami w sieci to tylko jedna z przyczyn, poprzez które prawo finansowe związane jest z Internetem. Z Internetu korzystają tak podatnicy (np. realizując transakcje) jak i organy podatkowe.

Zgodnie z artykułem 125 Ordynacji podatkowej<sup>131</sup> jedną z zasad postępowania organów podatkowych jest działanie wnikliwe, szybkie i osiągnięte dzięki najprostszym środkom, prowadzącym do załatwienia sprawy. Internet z uwagi na swoją charakterystykę doskonale nadaje się do prowadzenia postępowania podatkowego. Ordynacja podatkowa w dziale IV- postępowanie podatkowe- zawiera przepisy, którym sieć nadaje nowe znaczenie. Mowa tu o art. 150 § 2 przy zakwalifikowaniu elektronicznego wydania dziennika w zakres znaczeniowy „dziennika o zasięgu ogólnopolskim” , który został podany w przepisie<sup>132</sup>. Artykuł 160 dotyczy szczególnych form wezwania „przy użyciu innych środków łączności”. Bez żadnych wątpliwości możemy tu stwierdzić, że takim środkiem jest, na przykład, poczta elektroniczna.

W postępowaniu dowodowym organy podatkowe mogą posługiwać się zapisami na elektronicznych nośnikach informacji w myśl art. 180 ordynacji podatkowej. Najważniejszym jednak przepisem jest art. 168, określający sposoby wnoszenia podań i ich wymogi formalne. Ustawodawca obok telegrafu, dalekopisu i telefaksu wymienia także pocztę elektroniczną. Przepis ten na razie nie ma zastosowania w przypadku poczty elektronicznej z uwagi na trudności techniczne.

Polskie organy podatkowe wykorzystują sieć w dosyć ograniczonym stopniu. Na stronach WWW Ministerstwa Finansów<sup>133</sup> dostępne są, w formie plików, druki zeznań podatkowych. Znajdziemy tu także obowiązujące rozporządzenia podatkowe, inne akty prawne i komunikaty wydawane przez ministerstwo. Dodatkową informacją jest wykaz numerów telefonicznych urzędów skarbowych wraz z ich adresami z obszaru całego kraju, wykaz numerów rachunków bankowych urzędów skarbowych oraz raporty, dotyczące wpływów z podatków.

Spójrzmy jednak w przyszłość jak będzie za kilka lat wyglądał sposób płacenia podatków. Możemy to zrobić patrząc na rozwiązania zastosowane w Stanach Zjednoczonych<sup>134</sup>. Można tam składać zeznania podatkowe korzystając z 25 serwisów zaaprobowanych przez tamtejszą administrację podatkową. W 1999 r. Internal Revenue Service (urząd odpowiedzialny za ściąganie podatków, wchodzący w skład Departamentu skarbu USA) otrzymał drogą elektroniczną niemal 30 milionów zeznań podatkowych za rok 1998 (ze złożonych 125 milionów). Amerykanie mogli też informować o uzyskanych dochodach samodzielnie poprzez telefon, modem oraz Internet za pośrednictwem

---

<sup>131</sup> Ustawa z dnia 29.08.1997 r. Ordynacja podatkowa (Dz.U.97.137.926).

<sup>132</sup> Rozważania na temat prasy w Internecie zawarte zostały z rozdziale 3.3. pracy magisterskiej pt. prawo prasowe.

<sup>133</sup> <http://www.mf.gov.pl>

<sup>134</sup> Informacje można zacytować ze strony amerykańskiego departamentu skarbu: <http://www.ustreas.gov/>, na temat elektronicznych rozliczeń podatkowych w Holandii zobacz: R. Zasuń, *Fiskus królowej Beatrycze*, „Gazeta Wyborcza” z 11.12.2000.

autoryzowanych firm podatkowych<sup>135</sup>. Inną zaletą jest regulowanie należności przez podatników za pomocą karty płatniczej. Istnieją serwisy, gdzie można skonsultować się z doradcą podatkowym.

Internet to nie tylko szybkość i sprawność- nowa jakość w postępowaniu podatkowym. To także obniżka kosztów postępowania<sup>136</sup> oraz zwiększenie skuteczności i niezawodności systemu. Takie są kierunki, w których w niedalekiej przyszłości będzie zmierzał polski system podatkowy<sup>137</sup>.

Internet oferuje dla podatników szereg „miejsc” (stron WWW), dzięki którym uzyskać można wiele ważnych informacji (strony poświęcone są poszczególnym podatkom jak i całemu systemowi)<sup>138</sup>. W związku z obrotem handlowym w sieci nasuwają się pytania dotyczące zasad opodatkowania tego rodzaju transakcji i to zarówno w obrocie wewnętrznym jak i międzynarodowym. Pytania te dotyczą, przede wszystkim, podatku VAT (w USA tzw. *sales tax*), kryteriów rozróżniania usług, towarów i dóbr niematerialnych oraz możliwości omijania obowiązków podatkowych ze względu na lokalizację serwera<sup>139</sup>.

Ważną kwestią jest ustalenie systemu, dotyczącego podatków w Internecie. Czy wprowadzić nowy podatek czy też cały nowy system?<sup>140</sup> Czy też adaptować już istniejące rozwiązania w stosunku do Internetu? Czy może pozostawić Internet wolny od podatków? W prasie toczy się dyskusja na temat opodatkowania Internetu.<sup>141</sup> Unia Europejska w dokumencie a European Initiative in Electronic Commerce<sup>142</sup> przychyliła się do postulatu zapewnienia dla handlu elektronicznego czystego i neutralnego podatkowego otoczenia. Jednak w samej Unii Europejskiej istnieje system podatkowy, który nie jest jeszcze zunifikowany. Największym problemem jest uregulowanie prawne dotyczące podatku w sieci w USA. Obecnie wszystkie zakupy w sieci są zwolnione od podatków. Tak będzie do końca października 2001 roku, gdyż dopiero wtedy wygasa rządowe moratorium otaczające Internet ochroną przed opodatkowaniem<sup>143</sup>. Rozwiązanie takie powoduje zachwianie równowagi między firmami z Europy i ze Stanów Zjednoczonych. Pierwsze muszą bowiem płacić podatek VAT, te drugie są z tego obowiązku zwolnione (pamiętajmy, że mowa tu oczywiście o firmach elektronicznych, czy też zawierających transakcje elektroniczne).

Pojawiają się także problemy klasyfikacji określonych transakcji (do świadczenia usług czy do umowy sprzedaży na przykład). Wielka Brytania przyjmuje inne zasady stosowania podatku VAT do transakcji „elektronicznej” i „papierowej”. Stosownie do regulacji obowiązującej w Zjednoczonym Królestwie, udostępnienie książki za pośrednictwem Internetu, dokonane w ramach tego kraju

<sup>135</sup> M. Adamczyk, *Elektroniczny podatek*, tygodnik „Wprost” z 16.04.2000, s.6-7.

<sup>136</sup> Ibidem.

<sup>137</sup> W Polsce w 2001 roku Izba Skarbowa w Szczecinie uruchomiła pilotażowy projekt składania zeznań podatkowych PIT i CIT drogą elektroniczną. Bierze w nim udział około 40 osób fizycznych i prawnych. Zob. A.my, *PIT wysłany mailem*, „Rzeczpospolita” z dn. 20.04.2001.

<sup>138</sup> Na przykład: <http://www.pit.pl/>, <http://www.vat.pl/>

<sup>139</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 314-315.

<sup>140</sup> A. Surdacka-Oberbeck, *Zarys problematyki podatkowej w Internecie*, [w:] R. Skubisz, *Internet – problemy prawne*, op. cit., s.151.

<sup>141</sup> Gerald E.Seib, Jim Vandehei, *Amerykańskie pospolite ruszenie na rzecz opodatkowania sieci*, Wall Street Journal, przetłum. przez J. Skup, „Gazeta Wyborcza” z 03.07.2000 r., zob. też J. Palarczyk, *Jak podzielić złote jajo*, „Gazeta Wyborcza” z 09.03.2000 r.

<sup>142</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 315.

<sup>143</sup> J. Palarczyk, *Jak podzielić złote jajo*, op. cit.

lub innego państwa UE, związane jest z zapłaceniem VAT-u. Gdy jednak ta sama transakcja dotyczy „papierowej” książki, w zasadzie obowiązuje zwolnienie podatkowe. Wiąże się to, między innymi, z różnym traktowaniem, dla celów podatkowych, sprzedaży towarów i świadczenia usług; przy zaliczeniu udostępnienia informacji lub powieści do świadczenia usług<sup>144</sup>.

Ciekawym problemem jest także ustalenie czy opodatkowanie powinno być dokonywane w siedzibie dostawcy czy też odbiorcy. Z uwagi na immanentną cechę Internetu, jaką jest globalizacja, wytworzenie stałych rozwiązań w tym przedmiocie jest konieczne. Tu również należy zwrócić uwagę na fakt, iż owe przyszłe rozwiązania będą musiały dotyczyć większości krajów (jeśli nie wszystkich), gdyż jakiegokolwiek wyjątki od wypracowanych schematów będą powodowały ich nieprzydatność i skuteczne omijanie przepisów<sup>145</sup>.

## Prawo bankowe

Rozwój sieci wpłynął na prawo bankowe i zakres usług świadczonych przez instytucje finansowe. Najważniejszą przyczyną, jak zawsze w przypadku banków, są pieniądze. Realizacja zlecenia za pomocą Internetu jest 100 razy tańsza od podobnej czynności dokonanej przy pomocy kasjera w okienku bankowym. Dużą rolę odgrywa tu satysfakcja klienta, szybkość usługi, jej indywidualizacja, zwiększenie zasięgu geograficznego oraz rozszerzenie zakresu oferowanych produktów<sup>146</sup>. Warunki te sprawiają, że Internet ma coraz większy wpływ na prawo bankowe.

Ważną instytucją w polskim systemie bankowym jest Narodowy Bank Polski. Także i on wykorzystuje Internet do prowadzenia swej polityki, dotyczącej nadrzędnego celu banku, którym jest utrzymanie stałego poziomu cen. Dzięki stronie WWW<sup>147</sup> banku centralnego możemy zapoznać się z jego strukturą, dowiedzieć się o jego Prezesie oraz pozostałych organach (Zarząd NBP i Rada Polityki Pieniężnej). Najważniejszy polski bank udostępnia internautom swoje publikacje (w formacie PDF) oraz wszelkie akty prawne związane z jego działalnością. Dostępne są także czytelne statystyki m.in. bilans systemu bankowego, wyniki sektora bankowego.

Zwiększenie i urozmaicenie zakresu usług bankowych stwarza nowe warunki na bankowym rynku. Pojawiają się elektroniczne odmiany tradycyjnych banków, nastawione na „elektronicznych” klientów.<sup>148</sup> Dziś bez komputerów i informatyki nie sposób sobie wyobrazić funkcjonowania normalnego banku. Za tymi zmianami technologicznymi i jakościowymi podąża także i prawo bankowe, przystosowując się do nowych warunków.

W artykule 7 ustawy prawo bankowe z dnia 29.08.1997 r. (Dz.U.97.140.939.) wprowadzono ważną regulację, znajdującą coraz większe zastosowanie w prawie bankowym. Oświadczenia woli składane w związku z dokonywaniem czynności bankowych mogą być wyrażane za pomocą elektronicznych nośników informacji.

<sup>144</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit. s. 319.

<sup>145</sup> Przenoszenie siedziby przedsiębiorstwa do tzw. rajów podatkowych.

<sup>146</sup> W. Chmiela, *Systemy elektronicznej bankowości i cyfrowej płatności*, Warszawa 1999, s.72-73.

<sup>147</sup> <http://www.nbp.pl/>

<sup>148</sup> A. Myczkowska, *Bank www*, „Rzeczpospolita” z 26.07.2000 r. oraz A. Myczkowska, *Rachunek w sieci*, „Rzeczpospolita” z 15.11.2000 r.

Dokumenty takie związane z czynnościami bankowymi powinny być jednak w należyty sposób utrwalone i zabezpieczone. Ważny jest ustęp 2 artykułu 7 który stwierdza: *Jeżeli ustawa zastrzega dla czynności prawnej formę pisemną, uznaje się, że czynność dokonana w formie, o której mowa w ustępie 1, spełnia wymogi formy pisemnej.* Przepis ten, mimo że w Polsce nie ma jeszcze ustawy o podpisie elektronicznym zrównuje formę elektroniczną transakcji z formą pisemną. Jest to o tyle ważne, że w polskim prawie to jedyny wyjątek. Uwzględnić należy jednak specyfikę transakcji bankowych oraz stopień informatyzacji tej gałęzi gospodarki.

Ustawodawca dopuszcza także dokonywanie bankowych rozliczeń pieniężnych (bezugotówkowych) za pomocą elektronicznych nośników informacji (art.63 ust.3 ustawy prawo bankowe). Oznacza to przykładowo, że polecenie przelewu może być wydawane również przy pomocy komputera (pocztą elektroniczną)<sup>149</sup>. Jednak w przypadku wypłat dokonywanych za pomocą elektronicznych nośników informacji musi być dokonane automatyczne sprawdzenie autentyczności personalnego numeru identyfikacyjnego bądź hasła albo obu tych danych (art. 65 ust.2 prawa bankowego).

Związków Internetu z prawem bankowym jest więcej. Z uwagi jednak na ramy niniejszego opracowania zmuszony jestem poprzestać jedynie na tych przeze mnie poruszonych.

## Pozostałe działy prawa finansowego

Technologiczne zmiany dotknęły również prawo walutowe i dewizowe. Coraz większy transfer towarów i usług w sieciach komputerowych stwarza konieczność znalezienia rozwiązania dla płatności za owe przekazy. Powstało kilka rozwiązań, które dotyczą e-pieniądza<sup>150</sup>. Oto one:

- *First Virtual* – system obsługi transakcji, oparty na kartach płatniczych i poczcie elektronicznej (podstawowe cechy systemu to m.in. unikalny numer kodowy tzw. *Virtual PIN*, konieczność potwierdzenia każdej transakcji),
- Elektroniczny portfel- *Cyber Cash Wallet*- umożliwia wykorzystanie trzech typów płatności:
  - kart płatniczych- *Secure Card Service*
  - elektronicznej gotówki *CyberCoin*
  - system elektronicznych czeków *PayNow*<sup>151</sup>,
- Elektroniczna gotówka- *Ecash* system anonimowej elektronicznej gotówki, działający w trybie *on line* (pieniądze są jednorazowe, posiadają określony nominał, numer seryjny i zabezpieczenie w postaci podpisu cyfrowego banku emitenta, generacja unikalnego identyfikatora) <sup>152</sup>.

<sup>149</sup> W. Pyziół, *Prawo bankowe- komentarz- praca zbiorowa*, Warszawa 1999, s. 105.

<sup>150</sup> Jednym z owych zagadnień jest kwestia elektronicznych instrumentów płatniczych. Trwają obecnie prace nad ustawą regulującą tę materię. Dotyczyłaby ona zasad wydawania i użytkowania elektronicznych instrumentów płatności (kart), prowadzenia działalności przez niebankowe instytucje wydające pieniądź elektroniczny (np. sieci sklepów), tworzenie nadzoru nad ową działalnością oraz zasad wydawania i zarządzania pieniądzem elektronicznym. Zob. A. Myczkowska, *Dobrze tylko dla banków*, „Rzeczpospolita” z 17-18.02.2001, oraz tejsze *Banki przejmują odpowiedzialność*, „Rzeczpospolita” z 09.02.2001.

<sup>151</sup> Tak np. na gruncie obowiązującego prawa czekowego przyjąć należy, iż niedopuszczalne jest wystawienie i wprowadzenie do obiegu czeku elektronicznego (czek musi mieć formę dokumentu pisemnego) Ibidem str.105.

<sup>152</sup> Patrz bliżej: W. Chmielarz, *Systemy elektronicznej bankowości i cyfrowej płatności*, op. cit , s. 47-58 oraz [www.digicash.com](http://www.digicash.com)

Elektroniczny system zagościł na stałe na giełdach papierów wartościowych. Obrót papierami wartościowymi na rynku kapitałowym odbywa się w Polsce wyłącznie w formie zdematerializowanej, wewnątrz elektronicznego systemu przetwarzania danych. Papiery wartościowe nie istnieją zatem w formie fizycznej, ale w postaci zapisów na kontach inwestorów<sup>153</sup>.

Internet daje jednak dużo większe możliwości. Jego zalety szybko dostrzeżono na giełdach. Powstały elektroniczne domy maklerskie, które poprzez sieć przyjmują zlecenia. Dzięki rachunkowi internetowemu można dokonywać przelewów środków pieniężnych z rachunku prowadzonego przez dom maklerski na inne rachunki. Możliwe jest przeglądanie historii i salda rachunku. Niektóre banki przysyłają drogą elektroniczną (*e-mail*, SMS) powiadomienia dotyczące rachunku inwestycyjnego oraz ważne informacje rynkowe. Niestety rozwój tego rodzaju usług w pewnym stopniu zależy również od decyzji administracyjnych<sup>154</sup>. W Internecie funkcjonuje poza tym duża liczba serwisów poświęconych papierom wartościowym. Jest to prawdziwa kopalnia wiedzy tak o spółkach, jak i innych podmiotach.

Ciekawym problemem będzie oddziaływanie Internetu na prawo dewizowe. Szereg coraz to nowych możliwości inwestowania kapitału poprzez sieć daje możliwość lokowania go tam, gdzie w danej chwili jest to najbardziej opłacalne. Globalizacja powoduje szybki przepływ kapitału i osiąganie maksymalnych zysków. Według prawa dewizowego, Polacy mogą kupować akcje emitowane przez zagraniczne spółki pod warunkiem, że ich siedziba znajduje się w kraju należącym do OECD (Organizacji Współpracy Gospodarczej i Rozwoju) albo takim, z którym Polska podpisała umowę o popieraniu i wzajemnej ochronie inwestycji<sup>155</sup>. Takie lokaty mogą być dokonywane wyłącznie za pośrednictwem polskich biur maklerskich, posiadających specjalne zezwolenie Komisji Papierów Wartościowych i Giełd. Jak polskie przepisy dotyczące prawa dewizowego wytrzymają konkurencję z Internetem, w czasach w których kapitał tak jak i sieć nie zna granic przekonamy się już niedługo.

Jednym z działów prawa finansowego jest prawo finansowe ubezpieczeń państwowych. Internet dotyczy nie tylko ubezpieczeń społecznych ale również majątkowych i osobowych. Zakład Ubezpieczeń Społecznych uruchomił program wymiany dokumentów ubezpieczeniowych przez Internet<sup>156</sup>. Dzięki programowi Płatnik Przekaz Elektroniczny możliwe jest przekazywanie w formie elektronicznej dokumentów poprzez ekstranet, Internet oraz CD-romy i dyskietki.

Nas interesuje, przede wszystkim przesyłanie dokumentacji za pomocą poczty elektronicznej. Na stronach ZUS-u możemy dokładnie dowiedzieć się o tym rozwiązaniu oraz zaopatrzyć się w najnowsze wersje programów (Program Płatnik Przekaz Elektroniczny wersja AT 2.02.003, AT 2.02.008). Ten sposób rozliczania z Zakładem kierowany jest na razie do przedsiębiorców lecz miejmy nadzieję, że dzięki sukcesowi owego rozwiązania stanie się on dostępny także i dla zwykłych obywateli.

---

<sup>153</sup> A. Majchrzycka-Guzowska, *Finanse i prawo finansowe*, op. cit., s. 251-252.

<sup>154</sup> KPWiG może nie pozwolić na zamieszczenie informacji w prospektach emisyjnych o składaniu zapisów w ofertach publicznych za pomocą sieci.

<sup>155</sup> K. Kuresz, *Papiery wartościowe przez Internet*, „Rzeczpospolita” z 26.07.2000 r.

<sup>156</sup> <http://www.zus.gov.pl/>

Nowe możliwości Internetu to również zawieranie umów poprzez sieć. Umowy ubezpieczenia majątkowego i osobowego dostępne w cyberprzestrzeni znacznie ułatwiają procedury oraz redukują koszty. Internet stwarza możliwość przesyłania dokumentacji celnej, wymiany informacji, lepszej kontroli oraz zmniejszenia kosztów funkcjonowania administracji.

Widzimy więc, że związki Internetu z prawem finansowym są rozległe. Postęp techniczny sprawia, że konieczne są zmiany przepisów prawnych. Tu także prawo powinno ułatwiać rozwój usług internetowych oraz tworzyć podstawy do bezpiecznego obrotu kapitałem.

Internet spełnia informacyjną rolę jeśli chodzi o tworzenie społeczeństwa kapitalistycznego. Stwarza równe szanse dla wszystkich obywateli w procesie gromadzenia informacji, a przecież to właśnie informacja jest dziś najlepszym towarem.

## Rozdział IV.

### Zastosowanie Internetu w polskim prawie prywatnym

#### 1. Prawo pracy

Dziedzina prawa, którą jest prawo pracy podlega nieustannym przeobrażeniom. Na stosunki społeczne będące jej podstawą wpływa wiele procesów zachodzących w życiu codziennym. Jedną z przyczyn owych zmian jest Internet. Nowa technologia ma ogromny udział w tworzeniu nowych miejsc pracy oraz w rozwoju gospodarczego świata. E- przedsiębiorstwa są nastawione na zaspokajanie potrzeb internautów oraz elektronicznego społeczeństwa. Sam komputer już dawno przestał być tylko narzędziem pracy, a stał się raczej multimedialnym terminalem łączącym w sobie różne funkcje.

Informatyka wpływa na prawo pracy w dużym stopniu. W doktrynie trwa dyskusja nad nową wizją prawa pracy oraz nad kierunkiem zachodzących zmian. W podrozdziale tym przedstawię wpływ Internetu na normy prawne tej gałęzi prawa oraz wyzwania przed którymi stoi nauka przedmiotu w XXI wieku.

#### Przepisy kodeksu pracy a Internet

Komputeryzacja i informatyzacja stanowisk pracy stwarza ciekawe problemy w zakresie obowiązków pracowniczych (art. 100 k.p.). Jednym z nich jest przestrzeganie zasad bezpieczeństwa i higieny pracy (art. 100 §2 pkt 3). Czy zatem nieodpowiednie zabezpieczenie wejścia do systemu komputerowego będzie naruszeniem elementarnych zasad bezpieczeństwa? Czy niedbalstwo pracownika w materii haseł i kodów należy uznać za takie naruszenie?

Wydaje się, iż ze względu na wartość i znaczenie owych fundamentalnych zasad bezpieczeństwa sieci komputerowych podobne zachowanie powinno być rozumiane jednoznacznie jako zaniedbanie obowiązków. W razie powtarzających się naruszeń uzasadniałoby to rozwiązanie umowy o pracę bez wypowiedzenia z winy pracownika na podstawie art. 52 §1 pkt 2 k.p..

Analogiczne stanowisko zajął Sąd Najwyższy w sprawie Tomasza K., zwolnionego dyscyplinarnie za transfer z sieci danych stanowiących tajemnicę pracodawcy i dostępnych dopiero po wykonaniu określonego trybu poleceń.<sup>157</sup> Sąd Najwyższy zakwalifikował takie działanie jako naruszenie obowiązku pracownika zawartego w art. 100 §2 pkt 4 (dbanie o dobro zakładu pracy).

Innym obowiązkiem pracownika jest dochowywanie tajemnicy określonej w odrębnych przepisach (art. 100 §2 pkt 5 k.p.). W przypadku przechowywania na elektronicznych nośnikach informatycznych danych mających podstawowe znaczenie (często będącymi jedynym majątkiem przedsiębiorstwa, na którym wręcz opiera się jego działalność np. bazy danych) naruszenie owego obowiązku

---

<sup>157</sup> J. Lewandowska, *Ciekawość przyczyną zwolnienia*, „Rzeczpospolita” z dn. 26.02.2001 r.

jednoznacznie uzasadnia zwolnienie pracownika na podstawie art. 52 §1 pkt 1 (a często i pkt 2) w związku z artykułami 101<sup>3</sup>, 266, 267, 269 k.k..

Katalog obowiązków pracodawcy jest dużo bardziej rozbudowany. Jednak obowiązki te nie stwarzają aż takich problemów. Należy tu zwrócić, przede wszystkim, uwagę na organizację pracy zapewniającą pełne wykorzystywanie czasu pracy, osiąganie przez pracowników wysokiej wydajności i należytej jakości pracy przy wykorzystaniu ich uzdolnień i kwalifikacji (art. 94 pkt 2 k.p.).

Charakterystyczne jest także zagwarantowanie bezpieczeństwa i higienicznych warunków pracy (art. 94 pkt 3 k.p.). Przy pracy związanej z komputerem i jego obsługą powinno być to realizowane poprzez filtry ochronne i odpowiednio częste badania wzroku pracowników<sup>158</sup> oraz przerwy w pracy. Elementarnym obowiązkiem jest również ten przewidziany przez kodeks pracy w art. 94 pkt 1 – pracodawca powinien zaznajomić pracowników z systemem, hasłami dostępu oraz wszelkimi innymi charakterystycznymi dla określonego rodzaju pracy sposobami jej wykonywania. Jedną z podstawowych zasad prawa pracy głosi, iż pracodawca jest obowiązany szanować godność i inne dobra osobiste pracownika (art. 11<sup>1</sup> k.p. w związku z artykułami 23 i 24 k.c.).

Z zagadnieniem tym wiąże się problem jawności korespondencji (*e-maili*) pracowników i jej przeglądanie przez pracodawcę. Wiele firm prowadzi obsługę *mail box'ów* pracowników na własnych serwerach czy też poprzez usługi zlecone innym firmom. Problem kontrolowania *e-maili* pracowników jest zagadnieniem znaczącym. Chodzi tu o określenie swobody wkraczania pracodawcy w dobra osobiste pracowników<sup>159</sup>. Zwrócić należy tylko uwagę, iż kwestia ta różnie uregulowana jest w poszczególnych krajach (np. w Wielkiej Brytanii pracodawca posiada prawo przeglądania korespondencji pracownika).

Prawo pracy nie pozostaje wolne od wpływu podpisu elektronicznego. Tak jak i w innych gałęziach tak i tu podpis elektroniczny zrównany jest pod kątem skutków prawnych (pamiętajmy że nastąpi to w momencie wejścia w życie ustawy o podpisie elektronicznym) z podpisem odręcznym. Szereg przepisów kodeksu pracy dotyczących formy pisemnej (np. artykuły 29, 68<sup>2</sup>, 70 §1, 70 §1<sup>1</sup>) uzyska nowy wymiar. Podpis umożliwi w dużo większym stopniu odpersonalizowanie stosunku pracy. Zaistnieją sytuacje, w których pracodawca od początku do końca (od podpisania umowy o pracę do momentu jej rozwiązania) będzie miał jedynie wirtualny kontakt z pracownikiem.

Taki stan rzeczy wpłynie zdecydowanie na rozwój elektronicznych przedsiębiorstw oraz na warunki panujące na rynku pracy. Innego znaczenia nabiorą także nowe formy zatrudnienia. Jedną z nich jest telepraca.

## Telepraca

---

<sup>158</sup> A. Chobot, *Nowe formy zatrudnienia*, Warszawa 1997, s. 167.

<sup>159</sup> J. Wojciechowski, *Despotom nie*, „Rzeczpospolita” z dnia 28.11.2001 r.

Jak zauważa Andrzej Chobot w książce *Nowe formy zatrudnienia*<sup>160</sup> każda definicja musi brać pod uwagę różnorakie czynniki. Skonstruowanie definicji telepracy jest o tyle trudne, że jest to zjawisko nowe oraz do końca jeszcze nieukształtowane. Cały czas pojawiają się nieznane rozwiązania a i przepisy ustawowe różnie traktują tą kwestię. Czynniki, które należy uwzględnić są:

- lokalizacja stanowisk pracy,
- proporcje czasu poświęconego telepracy,
- lokalizacja stanowisk pracy,
- rodzaj stosowanej technologii,
- czy też wyłączność stosunku z pracodawcą.

W zależności od podejścia do określenia telepracy można stworzyć definicje szerokie lub wąskie. Definicja szeroka mogłaby być rozciągnięta tak aby kwalifikować w swój zakres pracy tzw. białe kołnierzyki (*white collar workers*). Wąskie definicje odnoszą się tylko do stosunku pomiędzy pracodawcą (zakładem pracy o charakterze biura) i odległym od niego przestrzennie pracownikiem, który ma formalny status stałego pracownika<sup>161</sup>. Należy pamiętać, że termin ów może być stosownie rozszerzony poprzez włączenie szeregu innych typów stosunku umownego.

Kolejną zmienną jest proporcja czasu spędzonego przez pracownika na wykonywanej pracy poza siedzibą pracodawcy. Występują tu dwa skrajne modele. W pierwszym z nich pracownik całość pracy wykonuje poza siedzibą przedsiębiorstwa. W drugiej natomiast jest to kontakt czysto przypadkowy spowodowany opóźnieniem w dotarciu do pracy (określa się takich pracowników mianem *cichych telepracowników*). Ze względu na rodzaj stosowanej technologii coraz bardziej powszechny jest Internet i Intranet (sieć wewnętrzna). To one zasadniczo zmieniają oblicze firm tak starej gospodarki jak i *e-biznesu*.

Kolejnym czynnikiem jest lokalizacja stanowisk pracy. W tym przypadku możemy rozróżnić stanowiska pracy w domach pracowników i w tzw. centrach informatycznych- *telecottages*. Podkreślić należy, iż wraz z rozwojem technik komputerowych (np. dostępność *lap top'ów*- mobilnych komputerów) jednoznaczne określenie miejsca wykonywania pracy będzie miało marginalne znaczenie, gdyż pracownik pracę może wykonywać praktycznie wszędzie (np. w podróży na lotnisku czy nawet w samolocie, w restauracji, kawiarni itd.). Pozostaje jeszcze kwestia wyłączności stosunku z pracodawcą. Niektóre definicje telepracy zawężają ją do przedsięwzięć, w których pracownik w całości jest zatrudniony (albo w większości) u jednego pracodawcy. Inne definicje uwzględniają przedstawicieli wolnych zawodów.

Jak widzimy problemy z ustaleniem definicji telepracy są duże. Ogólnie można ją jednak określić jako: formę zatrudnienia, która zakłada, że pracownik nie będzie wykonywał czynności zawodowych tylko w firmie ale będzie miał z nią kontakt za pomocą wszelkich dostępnych środków łączności. Literatura wyróżnia kilka podstawowych typów telepracy. Są to mianowicie:

1. telepraca domowa (*home-base work*) przy czym dzieli się ona na trzy odmiany:

---

<sup>160</sup> A. Chobot, *Nowe formy zatrudnienia*, op. cit., s. 160.

<sup>161</sup> Ibidem, s.161.

- praca domowa wykonywana częściowo w domu częściowo w lokalu przedsiębiorstwa
- telepraca domowa wykonywana w pełnym wymiarze dla jednego pracodawcy
- praca w całości w domu lecz przez osoby wykonujące wolny zawód, inaczej wolna praca domowa,
- 2. telepraca ruchoma (*mobile teleworking*),
- 3. telepraca w oddalonych miejscach kontrolowanych przez pracodawcę,
- 4. telepraca w *telecottages* albo w telecentrach,
- 5. praca wykonywana w ramach sieci informatycznej między przedsiębiorstwami<sup>162</sup>.

Sam system telepracy, abstrahując już od konkretnej jego formy czy definicji, powoduje wiele skutków w stosunkach gospodarczych jak i społecznych.

Możemy wyróżnić korzyści jakie niesie ze sobą telepraca oraz zagrożenia, które niewątpliwie należy wyeliminować w celu powszechniejszego stosowania tej formy zatrudnienia. Do najważniejszych zalet możemy zaliczyć obniżenie kosztów utrzymywania biura poprzez tworzenie stanowisk pracy w domach pracowników oraz możliwość znacznego zmniejszenia kosztów działalności samego przedsiębiorstwa poprzez zatrudnianie pracowników z tych rejonów kraju (świata), gdzie koszty pracy są niższe (czyli gdzie bezrobocie jest wyższe czy też oczekiwania płacowe pracowników stoją na niższym poziomie).<sup>163</sup> Inną dodatnią stroną telepracy jest ułatwianie relokacji pracy zwłaszcza w rejonach zacofanych ekonomicznie. Zdaniem A. Chobota telepraca sprzyja także regeneracji terenów, na których środowisko naturalne zostało zdewastowane przez tradycyjny przemysł wydobywczy i produkcyjny<sup>164</sup>. Telepraca zwiększa także możliwość zatrudnienia osób niepełnosprawnych czy też takich, które nie mogą wykonywać pracy poza miejscem zamieszkania (np. kobiety w ciąży czy w okresie macierzyństwa). Nowa forma zatrudnienia zmniejsza konsumpcję energii oraz stopień zanieczyszczenia środowiska<sup>165</sup>. Redukuje również koncentrację ludności w dużych miastach. Inną kwestią jest rozwój nowych gałęzi usług takich jak *e-banking*, *e-commerce* czy też telemedycyna.

Telepraca może skutkować także zmniejszaniem konfliktów międzyludzkich poprzez atomizację grup pracowniczych. Ta jednak zaleta staje się i wadą telepracy. Rozbijanie więzi międzyludzkich oraz alienacja jednostek jest dużym zagrożeniem dla społeczeństwa zdaniem A. Chobota<sup>166</sup>. Zaniepokojone tą sytuacją są zwłaszcza związki zawodowe. Niechęć też budzi niepewność zatrudnienia oraz możliwy wyzysk słabszych pracowników.

Nie podzielałbym jednak wszystkich tych obaw. Sam rozwój Internetu wcale nie spowoduje zamykania się ludzi w swych domach. Nie spowoduje także zwiększenia obojętności na sprawy życia codziennego. Tu gdzie upatruje się

<sup>162</sup> Podział przytoczony za A. Chobotem, *Nowe formy zatrudnienia*, op. cit, s.164-165.

<sup>163</sup> G. Raszkowska, *Nie w biurze i nie na etacie*, „Rzeczpospolita” z dn. 13.12.2000 r.

<sup>164</sup> A. Chobot, *Nowe formy zatrudnienia*, op. cit., s.156.

<sup>165</sup> Alvin Toffler w Trzeciej fali wyliczył, iż gdyby tylko 14 % pracowników (w USA) przestało dojeżdżać do pracy Stany Zjednoczone zaoszczędziłyby 34 mld dolarów, gdyż nie musiałyby importować ani kropli ropy naftowej.

<sup>166</sup> Ibidem, s. 157.

zagrożeń dostrzec można i szanse. Sieć korzystnie wpływa na stosunki międzyludzkie. Zwiększa znacznie edukację jednostek tak polityczną jak i społeczną. Stwarza możliwość czynnego udziału w życiu publicznym oraz zawodowym.

Informacja, która jest fundamentem informatycznego społeczeństwa otwiera ogromne perspektywy jeśli chodzi o rozwój więzi społecznych. Niepokojące, według mnie, jest zwłaszcza zjawisko globalizacji (dotyczy to również pracy). Przerzucanie i inwestowanie kapitałów w regiony o niskich kosztach produkcji może zapewnić im krótkotrwały wzrost gospodarczy obliczony jednakże na wykorzystanie aktualnych warunków oraz ucieczkę kapitału do innego regionu pozostawiając nierozwiązane problemy w danym środowisku. Innym zagrożeniem jest tworzenie się dwóch światów podzielonych stopniem zastosowania wszystkich możliwości Internetu. Świat podzielony na kategorie A i B (czasami i C) będzie dużo bardziej spolaryzowany majątkowo niż obecnie.

Mądre i właściwe wykorzystanie wszystkich szans jakie daje nowa technologia może te różnice zmniejszyć. Nie należy zapominać, iż krajom biedniejszym potrzebna jest pomoc w dostosowaniu ich gospodarek do nowych warunków e- świata.

Nowa wizja prawa pracy oparta jest, przede wszystkim na uelastycznianiu pracy. Literatura podkreśla duże znaczenie telepracy w tej materii<sup>167</sup>. Prawo pracy stoi przed wieloma problemami, które będą pojawiać się wraz z upowszechnianiem się telepracy. Przedsiębiorstwa wirtualne, oparte na sieci i nie będące klasycznymi podmiotami gospodarczymi spowodują wiele kłopotów interpretacyjnych.

E- gospodarka będzie także wymuszać na ustawodawcy dostosowanie przepisów do zmieniającej się rzeczywistości. Wraz z rozwojem oraz wzmacnianiem jej pozycji naciski te staną się coraz bardziej skuteczne. Internet znajduje zastosowanie nie tylko w telepracy. Firmy już od dawna wykorzystują go do prowadzenia szkoleń.

Szkolenia tradycyjne są poprzedzane kursami w trybie *on line*, by wyrównać poziom grupy <sup>168</sup>. Sieć stwarza możliwość lepszego kontaktu pracownika z pracodawcą. Staje się on bardziej bezpośredni i otwarty. Przepływ informacji w przedsiębiorstwach dużo zyskuje przy zastosowaniu Internetu ( czy też Intranetu). Można mówić o prawdziwej rewolucji w działach personalnych firm. Portale internetowe stwarzają możliwość realizacji szkoleń, umożliwiają dostęp pracownikom do ich teczek (a raczej plików), udzielania informacji o wynagrodzeniach czy też wszystkich procesach dokonujących się w przedsiębiorstwie. Nowego oblicza nabiera samo poszukiwanie pracy. W sieci jest ono łatwiejsze, tańsze oraz skuteczniejsze (można wszak bezpośrednio dowiedzieć się wszystkiego o danym miejscu pracy czy też wysłać swe podanie).

Z przedstawionych, przeze mnie, zagadnień związanych z Internetem w prawie pracy wynika jeden podstawowy wniosek. Internet będzie w coraz większym stopniu oddziaływał na tą dziedzinę prawa prywatnego. Można powiedzieć, że będzie to proporcjonalne do wzrostu znaczenia całego sektora e- gospodarki. Najbliższe lata przyniosą zmiany ustawowych przepisów, nowe

---

<sup>167</sup> A. Chobot, *Nowe formy zatrudnienia*, op. cit., s. 204-205 .

<sup>168</sup> G. Raszewska, *Nie w biurze i nie na etacie*, op. cit.

podejście do problemu Internetu i pracy. Czekają nas ciekawe rozwiązania w tej materii. Dziś już możemy stwierdzić, że prawo pracy nie pozostanie w dobie Internetu takie samo.

### 3. Prawo cywilne materialne

Postęp techniczny w dziedzinie informatyki determinuje zmiany w systemach prawnych. Nowe zjawiska w Internecie mają wpływ także na prawo cywilne – tak materialne, jak i procesowe<sup>169</sup>. Ustawodawca wprowadza nowe przepisy, doktryna i orzecznictwo nową wykładnię już istniejących. Zwiększający się obrót handlowy towarami i usługami w sieci oraz rosnąca ilość umów zawieranych w Internecie powodują narastanie wątpliwości, nieporozumień i konfliktów pomiędzy stronami umów cywilnych. Idąc z duchem czasu prawo przyswaja sobie dotąd nieznaną instytucję. W samej sieci tworzą się powszechnie akceptowalne zachowania, które już wkrótce przerodzą się w zwyczaje. Warto więc przyjrzeć się tej dziedzinie prawa, aby zobaczyć do jakich zmian przyczynia się Internet.

#### Oświadczenie woli

Jedynym koniecznym elementem każdej czynności prawnej, a zarazem wyłącznie charakteryzującym czynności prawne jest oświadczenie woli<sup>170</sup>.

Przejdźmy więc do analizy oświadczenia woli skoro jest ono tak niezmiernie ważne w prawie cywilnym. Możemy wyróżnić dwie jego specyficzne formy. Pierwszą jest sytuacja, w której oświadczenie woli pochodzi bezpośrednio od osoby lecz przekazywane jest (przesyłane i składane) za pośrednictwem np. Internetu. Zastosowanie tu znajdzie art. 60 k.c. Drugi przypadek wiąże się z automatyczną wymianą danych EDI (*Electronic Data Interchange*). System informatyczny niejako bez udziału człowieka składa i przyjmuje oświadczenia woli. Jak jednak w pracy *Internet a prawo* autorzy słusznie podkreślają komputer w pierw w został zaprogramowany przez człowieka i wykonuje tylko jego polecenia<sup>171</sup>.

Samo posługiwanie się komputerem/Internetem przy oświadczeniu woli wiąże się z innymi wątpliwościami. Jedną z nich jest uchylenie się od skutków oświadczenia woli z powodu błędu. Kodeks cywilny reguluje tę kwestię w artykułach 82-88. Kiedy wprowadzenie złych danych do systemu można uznać za błąd w rozumieniu art. 84 k.c.? Czy możemy zakwalifikować niewłaściwe funkcjonowanie programu komputerowego (które powoduje zmianę przesyłanych danych) jako zniekształcenie oświadczenia woli przez tzw. posłańca (art.85 k.c.)?

---

<sup>169</sup> Reakcją na postęp techniczny jest na przykład zakładanie i prowadzenie ksiąg wieczystych w systemie informatycznym. Art.25 {1} ust.2 ustawy o księgach wieczystych i hipotece (Dz.U. Nr 19 poz 147 z 1991 r. Nr 22, zmieniona ustawą z 15.03.2001 r. o zmianie ustawy o księgach wieczystych (...))

<sup>170</sup> Z. Radwański, *Prawo cywilne- część ogólna*, Warszawa 1999, s.194.

<sup>171</sup> Szerzej na ów temat J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.50-51.

Dotychczas dwa zasadnicze elementy oświadczenia woli – „akt woli” i jego „uzewnętrznienie” zbiegały się w czasie oraz odbywały się z udziałem czy pod bezpośrednią kontrolą osoby składającej oświadczenie<sup>172</sup>. Internet zmienia w zasadniczy sposób dotychczasowe konwencje. Pamiętajmy, iż oświadczenia woli składane poprzez sieć zasadniczo są oświadczeniami składanymi drugiej osobie. Znajdzie więc tu zastosowanie art. 84 k.c. Nie będzie można uznać za błąd zachowania w pełni świadomego, gdy składający w istocie nie znał jego treści. Nie jest również błędem samo wyciągnięcie fałszywych wniosków czy brak wyobrażenia co do skutków swego postępowania<sup>173</sup>.

Inną kwestią jest podszywanie się pod kogoś innego w celu złożenia oświadczenia woli. Osoba, która takiego oświadczenia nie złożyła i nie wiedziała o takim zachowaniu nie będzie odpowiedzialna. Jak podnoszą słusznie J.Barta i R.Markiewicz w pracy *Internet a prawo* należy zastanowić się nad uwzględnieniem interesów osób, które są adresatami „fałszywych oświadczeń woli”. W tej materii da się jednak zażegnać podstawowe rozbieżności z momentem wprowadzenia podpisu elektronicznego, który zapewni dużo większe bezpieczeństwo obrotu handlowego w sieci niż jest obecnie. W związku z tym, iż większość oświadczeń woli przekazywanych przez Internet ma charakter oświadczeń składanych drugiej osobie pojawia się problem momentu, w którym takie oświadczenie zostało złożone.

Spośród różnych teoretycznie możliwych koncepcji rozwiązań (teoria oświadczenia woli, teoria wysłania, zapoznania się z treścią, teoria doręczenia) prawo polskie stanęło na stanowisku tej ostatniej, tj. teorii doręczenia<sup>174</sup>. Samo dojście oświadczenia nie jest jeszcze skuteczne, gdyż jak przewiduje kodeks cywilny (art. 61) potrzebna jest jeszcze okoliczność, aby adresat mógł się zapoznać z jego treścią.

Wszelkie przeszkody, usterki w działaniu sieci informatycznej czy całego systemu obciążają w rozumieniu k.c. nadawcę. Możemy jednak postawić dwa pytania. Czy do złożenia oświadczenia woli dochodzi w momencie gdy dane przeszły przez modem odbiorcy, chociażby nie zostały zapisane? Czy też koniecznym elementem odebrania oświadczenia jest jego zapisanie? Doktryna przychyliła się bardziej do tego drugiego stanowiska. Lecz zauważmy tutaj, że istnieją poważne wątpliwości.

Nie możemy zapominać o interesie nadawcy oświadczenia woli. Wyróżnić należy szczególne zdarzenia gdy przyczyny niedojścia lub opóźnienia dojścia oświadczenia są tylko po stronie odbiorcy (przykładem może tu być zawirusowanie komputera i wiążąca się z tym jego niesprawność) w sytuacji gdy nadawca o nich nie wiedział. W takim przypadku adresat nie może powoływać się na fakt, iż oświadczenie nie doszło do niego w odpowiednim czasie. Zupełnie inaczej należy rozpatrywać moment otrzymania oświadczenia woli w systemie EDI<sup>175</sup>. Stanowisko nauki dotyczące możliwości wyłącznego składania oświadczenia woli przez Internet (np. poprzez pocztę elektroniczną) jest różne. Autorzy pracy *Internet a prawo* są zdania, iż takie umówienie się dotyczące

---

<sup>172</sup> Ibidem, s.51-52.

<sup>173</sup> Tak B. Lenarkiewicz – Petrykowska [w:] *System prawa cywilnego tom I, część ogólna*, Wrocław, Warszawa, Gdańsk, Łódź 1985, s.670.

<sup>174</sup> *Kodeks Cywilny Komentarz Tom I* pod red. K. Pietrzykowskiego, Warszawa 1999, s.210.

<sup>175</sup> Szerzej na ów temat: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.56.

komunikowania się poprzez sieć w razie niedochowania formy wiąże się z bezskutecznością czynności prawnej i jest niedopuszczalne<sup>176</sup>. M. Safian w komentarzu do k.c.<sup>177</sup> uważa, iż strony mogą urządzić ów sposób porozumiewania się i składania oświadczeń woli. Będzie on dla nich wiążący dla ustalenia czy doszło do skutecznego złożenia oświadczenia woli. Kwestia ta, jak i wiele innych tylko zasygnalizowanych przez mnie, w najbliższym czasie zapewne zostanie rozwiązana.

## Zawieranie umów przez Internet i ich rodzaje

W Internecie dochodzi do zawierania umów cywilnoprawnych. Jak więc z punktu widzenia prawa cywilnego scharakteryzować te umowy? Na wstępie wypada zaznaczyć, iż jest to temat o tyle obszerny, iż głęboka jego analiza wymagałaby oddzielnej pracy. W literaturze<sup>178</sup> możemy się spotkać z podstawowym podziałem na:

- typowe umowy *on-line* (dotyczą one specjalistycznych usług *on line*),
- atypowe umowy *on line* (dotyczą zwykłych kontraktów np. umów sprzedaży tylko realizowanych poprzez sieci komputerowe).

Wśród pierwszej grupy możemy przykładowo wyróżnić takie umowy jak:

- korzystanie z baz danych,
- przekazywanie poczty elektronicznej (*e-mail*),
- udostępnianie miejsca (w pamięci komputera, na serwerze) do przechowywania danych,
- kupno informacji,
- umożliwianie dostępu do Internetu,
- czy też sprzedaż *software* lub *hardware*.

Do dużej części podobnych umów będą miały zastosowanie przepisy o umowie o dzieło czy zlecenia. Wiele innych umów będzie rozpatrywanych (dotyczące nowo pojawiających się usług) jako umowy nienazwane. Pamiętajmy również, że ze względu na sposób spełnienia świadczenia będziemy mogli wyróżnić takie umowy jak:

- a) zawierane i realizowane wyłącznie w sieci,
  - b) zawierane w sieci lecz ich wykonanie następuje poza siecią (np. sprzedaż artykułów żywnościowych w Internecie),
  - c) oraz trzecie możliwość- zawierane poza siecią a realizowane w sieci (różne typy usług oraz sprzedaż produktów niematerialnych).
- Ów drugi podział będzie mieć duże znaczenie w przypadku umów sprzedaży.

Kodeks cywilny przewiduje trzy zasadnicze sposoby zawierania umów. W drodze:

---

<sup>176</sup> Ibidem s. 56-57.

<sup>177</sup> M. Safian, *Kodeks Cywilny Komentarz Tom I* pod red K. Pietrzykowskiego, op. cit., s. 211.

<sup>178</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 89.

- oferty,
- przetargu<sup>179</sup>,
- rokowań<sup>180</sup>.

Ten ostatni sposób ma duże szanse rozwoju. Klasyczne przetargi w Internecie chyba (gdyż trudno jest objąć wszystkie wydarzenia zaistniałe w sieci) jeszcze nie zaistniały (choć możemy powiedzieć, że w niedalekiej przyszłości na pewno znajdują się w cyberprzestrzeni).

W większości przypadków do zawarcia umowy dochodzi na podstawie złożenia oferty (czy też ofert). Wola zawarcia umowy określona w oświadczeniu woli wraz z jej istotnymi postanowieniami to oferta według art. 66 §1 k.c. Oświadczenie to może zostać skierowane do określonej osoby jak i do nieograniczonego kręgu osób (*ad incertas personas*). Taka oferta jednak może być w każdej chwili cofnięta. Oferent może ograniczyć czas związania ofertą (określić termin początkowy jak i końcowy).

Od oferty odróżnia się sytuację określaną jako zaproszenie do składania ofert i zaproszenie do rokowań. W razie wątpliwości, jak przewiduje to art. 71 k.c., oferty powinny być traktowane jako ogłoszenia, reklamy, cenniki i inne informacje skierowane do ogółu lub poszczególnych osób<sup>181</sup>.

Wyraźne rozgraniczenie oferty od cennika jest nad wyraz trudne w Internecie. Nie można jednoznacznie odpowiedzieć na to pytanie, gdyż moim zdaniem każdy przypadek należy rozpatrywać oddzielnie<sup>182</sup>. Ważna jest tu funkcja art. 543 k.c., który dodatkowo komplikuje sprawę. Czy zatem w myśl tego przepisu wystawienie rzeczy w miejscu sprzedaży na widok publiczny z oznaczeniem ceny jest ofertą w przypadku Internetu? Wbrew stanowisku J. Barty i R. Markiewicza, wyrażonym w pracy *Internet a prawo* jestem skłonny uznać takowe działanie za ofertę a nie za pewną kategorię ogłoszeń i reklam lecz tylko w przypadku towarów i usług w postaci niematerialnej (lit. a kryterium miejsca realizacji umowy).

W wielu przypadkach to użytkownik Internetu występuje w roli oferenta.<sup>183</sup> To on może składając ofertę określić procedurę jej przyjęcia a także podać wymagania co do formy i sposobu komunikowania się. W związku jednak z profesjonalizacją obrotu gospodarczego należy zauważyć, że w większości są to umowy adhezyjne, w których kupującemu pozostawiono bardzo niewielkie pole manewru.

Przejdźmy do zagadnienia wiążącego się z przyjęciem oferty czyli z uzyskaniem konsensusu. Ważną kwestią jest związanie stron ofertą. Łączy się z tym także konieczność ustalenia czy kontrakt zawarty został między obecnymi (*inter praesens*) czy też między nieobecnymi (*inter absents*). W drugim przypadku oferta przestaje wiązać z upływem czasu potrzebnego adresatowi w zwykłym toku czynności na zapoznanie się z jej treścią i wysłanie odpowiedzi bez

<sup>179</sup> Por. A. Stosio, *Kto kliknie więcej*, Rzeczpospolita z 03.01.2000 r. oraz M. Świerczyński, *Jak napój z automatu*, „Rzeczpospolita” z 30.11.2000 r.

<sup>180</sup> Powstaje pytanie jak zakwalifikować transakcje zawierane przez użytkowników Internetu np. poprzez strony WWW eBay.com. Przychylić się należy do zdania, iż zawierane są one w drodze rokowań.

<sup>181</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 57-58.

<sup>182</sup> W sieci funkcjonują sklepy detaliczne jak i supermarkety oferujące towary na podobnych zasadach jak w normalnych (czytaj niewirtualnych) punktach handlowych.

<sup>183</sup> Choć jak wiemy są także umowy zawierane między przedsiębiorcami – tzw. B2B – *biznes to biznes*.

nieuzasadnionej zwłoki<sup>184</sup>. W pierwszym wariantcie oferta przestaje wiązać, gdy nie została przyjęta niezwłocznie (oba przypadki reguluje art. 66 §2 k.c.)

Pojawia się problem czy Internet zakwalifikować w zakres wyrażenia ustawowego „innego środka bezpośredniego porozumiewania się na odległość”? I tu poglądy w literaturze są podzielone. Dostępne w Internecie tzw. *chat room'y* czy też inne aplikacje pozwalające na rozmowę w czasie rzeczywistym (o bezpośredniej rozmowie przez telefon czy komputer wyposażony w mikrofon i odpowiednie oprogramowanie nie wspomnę), moim zdaniem, mogą zostać zaliczone do tego zakresu.

Zdania w nauce przedmiotu, jak już powiedziałem są jednak podzielone. Związanie ofertą odmiennie przedstawia się w sytuacjach przewidzianych w art. 69 k.c. Ma to miejsce w przypadkach, gdy składający ofertę życzy sobie natychmiastowego wykonania umowy. Oferta przestaje wiązać w momencie gdy druga strona w czasie właściwym nie przystąpi do jej wykonania. Jak podkreślają autorzy pracy *Internet a prawo* użytkownik Internetu (oferent) jeśli nie uczynił odpowiedniej adnotacji w treści oferty, nie będzie mógł łatwo, a przynajmniej na razie, skrócić czasu związania ofertą, powołując się na wspomniany przepis i argumentując to brakiem niezwłocznego wykonania umowy. Jest tak dlatego, iż na razie trudno raczej mówić o „przyjętych zwyczajach” w odniesieniu do transakcji zawieranych poprzez Internet i to takich zwyczajach, które czynią zbędnym składanie oświadczenia o przyjęciu ofert.<sup>185</sup>

Pamiętajmy jednak o systemie EDI, w którym sam program „składa i przyjmuje” ofertę i powoduje wykonanie umowy. Ważnym zagadnieniem jest określenie czasu i miejsca zawarcia umowy, do której dochodzi na drodze przyjęcia oferty poprzez sieć. Potrzebne jest to w kwestiach proceduralnych (właściwość sądu) oraz praktycznych (stosowne zwyczaje).

Oczywiście strony same mogą oznaczyć czas i miejsce zawarcia umowy. W odmiennych uwarunkowaniach do złożenia oświadczenia woli dochodzi w różnym czasie i miejscu. Należy tu stosować jako wykładnię czasu i miejsca zawarcie umowy art. 70 k.c. Zatem chwilą zawarcia umowy będzie moment otrzymania przez składającego ofertę oświadczenia o jej przyjęciu przez oblata, względnie chwila przystąpienia przez drugą stronę do wykonania umowy. W kwestii miejsca zawarcia umowy, w razie wątpliwości, jest nim miejsce otrzymania przez składającego ofertę oświadczenia o jej przyjęciu, względnie miejsce zamieszkania składającego ofertę w chwili zawarcia umowy – art. 70 §2 k.c.

Z uwagi na globalny charakter Internetu nie możemy zapominać o przepisach prawa międzynarodowego prywatnego według których strony same mogą określić prawo właściwe dla zobowiązania. Tym też zagadnieniem zajmę się w dalszej części pracy poświęconej prawu cywilnemu.

## Forma pisemna

Aby zwiększyć bezpieczeństwo obrotu handlowego w Internecie należy wprowadzić szczególne formy zawierania umów w sieci. Są one zwięzieniem ogólnej zasady swobody umów z art. 60 k.c. Dotrzymanie określonej formy

<sup>184</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 60-61.

<sup>185</sup> Ibidem, s. 64.

pisemnej łączy się z określonymi skutkami (zastrzeżenie *ad solemnitatem, ad eventum* czy *ad probationem*). Wynikać ono może tak z ustawy jak i z porozumienia stron (art. 76 k.c.).

Jak daleko strony mogą posunąć się jednak z zastosowaniem takiej formy w kontaktach wzajemnych? Czy w grę będzie tu wchodzić także korespondencja np. *e-mail'ami*?

Uwagę należy zwrócić na §2 art. 74. Jest w nim mowa o dopuszczeniu dowodu, w przypadku nie zachowania formy pisemnej zastrzeżonej pod rygorem *ad probationem*, jeżeli „fakt dokonania czynności prawnej będzie uprawdopodobniony za pomocą pisma. Czy zatem wydruk komputerowy czy też zapis na elektronicznym nośniku informacji będzie takim uprawdopodobnieniem? W literaturze możemy dopatrzeć się stanowiska, iż takowa interpretacja byłaby przejawem wykładni rozszerzającej<sup>186</sup>. Wymóg dochowania formy pisemnej określony jest w art. 78 k.c. Na podstawie analizy tego przepisu możemy dojść do wniosku, iż dla zachowania tej formy potrzebne jest spełnienie dwóch warunków:

1. dokument musi być sporządzony w formie pisemnej (lecz nie musi być sporządzony własnoręcznie przez strony)
2. niezbędne jest własnoręczne złożenie podpisu pod dokumentem zawierającym treść oświadczenia woli.

**Ad 1.** Nauka przedmiotu podkreśla, iż dokument może być sporządzony np. na maszynie do pisania lub za pomocą innej techniki (wyjątkiem jest tu testament holograficzny). Nie musi być także sporządzony przez samego podpisującego lecz musi mieć walor trwałości.

Widzimy więc, że dokumenty elektroniczne owe przesłanki spełniają, gdyż trudno odmówić im waloru trwałości czy pisemności (i nie ma tu znaczenia fakt, iż są wyświetlane na ekranach monitorów).

**Ad 2.** Podpis musi służyć identyfikacji wystawcy oraz ma pozwolić na „powiązanie określonej osoby z treścią dokumentu”<sup>187</sup>

Wymóg identyfikacji trudno będzie spełnić w sieciach komputerowych bez zastosowania podpisu elektronicznego – jego materię przedstawię poniżej. Nie można przyjąć, iż przymiot „własnoręcznego podpisu” będzie miało wpisanie w edytorze tekstu imienia i nazwiska określonej osoby. Niemniej szuka się sposobów obejścia przepisów o formie pisemnej, aby na szerszą skalę posługiwać się dokumentami elektronicznymi. Problem dokumentów elektronicznych poruszyłem już w rozdziałach poświęconych prawu karnemu i finansowemu (dokładnie bankowemu). Wydaje się jednak, iż takie działania nie idą w dobrym kierunku i są tylko przejściowym rozwiązaniem. Rozwiązaniem, które czeka na ustawę o podpisie elektronicznym jako na sposób wprowadzenia ładu i bezpieczeństwa do obrotu handlowego w Internecie.

## Podpis elektroniczny

Istotą podpisu elektronicznego jest zrównanie go z podpisem własnoręcznym pod względem skutków prawnych. Musi on zakładać i spełniać dwa podstawowe warunki:

---

<sup>186</sup> Ibidem, s.66.

<sup>187</sup> Ibidem, s.67-68.

- dawać gwarancję, że dokument pochodzi od określonej osoby,
- zapewnić, że treść dokumentu oraz postawiony pod nim podpis nie zostały sfalszowane, przerobione czy podrobione.

Sam podpis elektroniczny może też zawierać znakowanie daty dokonania tej czynności. W tym sensie będzie on uwierzytelnieniem złożonego oświadczenia na wyższym nawet poziomie wiarygodności niż podpis odręczny<sup>188</sup>. Podpis elektroniczny ma wiele odmian. Jedną z nich jest podpis cyfrowy. Jego podstawy stworzyli w latach 70. dwaj matematycy i informatycy: Whitfield Diffie i Martis Hellman.

Istotą podpisu cyfrowego opartego na arytmetycznym systemie kodowania jest wykorzystanie dwóch różnych kluczy do podpisu.<sup>189</sup> Są to: klucz prywatny i klucz publiczny. Ten pierwszy stosowany jest przez podpisującego i jemu tylko dostępny, drugi natomiast jest publicznie dostępny. Pierwszy służy do szyfrowania, drugi jest kluczem deszyfrującym.

Zastosowanie klucza szyfrującego można porównać do złożenia przez podpisującego podpisu pod oświadczeniem woli. Klucz publiczny umożliwia sprawdzenie autentyczności danego dokumentu<sup>190</sup>. Zaznaczyć tylko należy, że powszechnie stosuje się do podpisu cyfrowego dwie metody – RSA (z kluczem 512 bitów oraz DSA – prywatne klucze wielkości 160 bitów a publiczne 1024 bitów<sup>191</sup>).

Co jednak rozumieć przez podpis elektroniczny? Przytoczę definicję podaną w art. 4 poselskiego projektu ustawy o podpisie elektronicznym z 05.12.2000 r.

*Podpisem elektronicznym są dane elektroniczne dołączone do innych danych elektronicznych lub logicznie z nimi powiązane w celu potwierdzenia tożsamości podmiotu podpisującego, który się nimi posługuje.*

Duże znaczenie w systemie podpisu elektronicznego będą mieli tzw. *certification- service providers*<sup>192</sup> czyli jednostki zaufania publicznego<sup>193</sup> wydające certyfikaty. Certyfikaty i system akredytacji mają służyć zapewnieniu bezpiecznego wydawania, stosowania i wycofywania z użytku podpisów elektronicznych.

Tak jak wyróżnia się podpis elektroniczny zwykły i kwalifikowany tak analogicznie przy systemie akredytacji możemy wyodrębnić dwa poziomy zaufania: bez akredytacji i z akredytacją. Podpis kwalifikowany używany by był w kontaktach z jednostkami sektora publicznego (organami i jednostkami pomocniczymi administracji rządowej, jednostkami samorządu terytorialnego, sądami, trybunałami, czy organami kontroli państwowej i NBP – projekt poselski – art.3 pkt 1).

Odrębną kwestią jest zagadnienie odpowiedzialności użytkownika klucza prywatnego. W przypadku wykorzystywania go przez osobę trzecią za zgodą uprawnionego należałoby tu zastosować przepisy o pełnomocnictwie. Lecz w razie

<sup>188</sup> I. Sitnicki, M. Srebrny, *Nie taki diabeł straszny jak go malują*, „Rzeczpospolita” z 08.02.2001 r.

<sup>189</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.71.

<sup>190</sup> Tworzenie podpisów cyfrowych opisane zostało dokładnie przez J. Stokłosę, *Techniczne i prawne aspekty podpisu cyfrowego w Internecie* [w]: R. Skubisz (red): *Internet- problemy prawne*, op. cit., s.119-130 oraz przez

<sup>191</sup> I. Sitnickiego i M. Srebrnego, *Nie taki diabeł straszny jak go malują*, op. cit.

<sup>192</sup> Pod skrótem RSA kryją się nazwiska twórców: Rivest, Shamir, Adelman.

<sup>193</sup> Za dyrektywą UE - Electronic Signatures Directive 99/93 z dnia 13.12.1999 r.

<sup>193</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.72.

wykorzystania przez osobę trzecią bez takiej zgody wyłącza się odpowiedzialność właściciela klucza bądź podmiotu przyznającego dany klucz.

Z uwagi na to, iż prace nad polską ustawą o podpisie elektronicznym trwają (w komisji sejmowej rozpatrywane są dwa projekty- rządowy i poselski) przedstawię unormowania w tej kwestii na świecie<sup>194</sup>.

Pierwszym dokumentem w tej dziedzinie był Utah Digital Signature Act z 1995 roku. Później za stanem Utah podążyły Kalifornia, Floryda, Illinois i Massachusetts<sup>195</sup>. W Europie pierwszą ustawą o podpisie cyfrowym (a nie elektronicznym) wprowadziły Niemcy- ustawa z 22.07.1997 r. o usługach informatycznych i komunikacyjnych, w której jako art. 3 zamieszczono obszerną ustawę o podpisie cyfrowym<sup>196</sup>. W ślad za Niemcami poszły kolejne kraje europejskie: Hiszpania (dekret królewski 14-99 z 17.09.1999 r.- ustawa o podpisie cyfrowym), Irlandia (The Electronic Commerce Act 2000), Czechy, Austria i Rosja (przepisy kodeksu cywilnego z 1996 r.). Parlament Europejski i Rada wydały dyrektywę dotyczącą podpisów elektronicznych (Electronic Signatures Directive 99/93 z dnia 13.12.1999 r.). Zakłada ona implementację przepisów dyrektywy przez państwa członkowskie do 19.06.2001 roku. Dyrektywa przewiduje istnienie dwóch rodzajów podpisów (zwykły i kwalifikowany), brak monopolu na usługi certyfikacyjne oraz pełną konkurencyjność na rynku tych usług (staną się one częścią e-biznesu). Przede wszystkim zrównuje podpis elektroniczny z podpisem własnoręcznym. Nie przesądza o strukturze, procedurach i technologiach potrzebnych do stosowania podpisu elektronicznego. Ważne są zawarte w niej definicje podstawowych pojęć z zakresu usług certyfikacyjnych i posługiwania się podpisami. Z uwagi na zbliżający się termin wdrożenia dyrektywy w życie przez państwa członkowskie trwają nieustanne prace dostosowawcze w krajach „15”. Polska ma szansę dostosować swe przepisy dotyczące podpisu elektronicznego do dnia 19.06.2001r.

Zainteresowanie podpisem elektronicznym nie kończy się jednak na systemach prawnych poszczególnych państw. Organizacje międzynarodowe włączyły się w proces unormowania tej kwestii m.in. Międzynarodowa Izba Handlowa -ICC, OECD, Komisja ONZ ds. Prawa Handlowego -UNCITRAL.<sup>197</sup>

Zaznaczyć należy, iż powstawanie szeregu przepisów w tej materii jest tylko pierwszym etapem procesu, który nieuchronnie będzie zmierzał do ujednoczenia przepisów oraz ich ogólnego stosowania, tak aby na mocy międzynarodowych porozumień i konwencji zagwarantować pełne bezpieczeństwo posługiwania się podpisem elektronicznym na całym świecie. Tu właśnie duże wyzwanie stoi przed organizacjami międzynarodowymi.

---

<sup>194</sup> Zob. odnośnie prac nad polską ustawą o podpisie elektronicznym: M. Manta, *Podpis elektroniczny- zarys przyszłych regulacji prawnych*, „Radca prawny” 02/53, 03-04 2001.

<sup>195</sup> W Stanach Zjednoczonych obowiązuje także ustawa federalna z 24.01.2000 r.- Electronic Signatures in Global and National Commerce Act.

<sup>196</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.73.

<sup>197</sup> Na temat działalności organizacji międzynarodowych, w tym Wspólnot Europejskich, w sprawie Internetu oraz o jego wpływie na prawo międzynarodowe piszę w osobnym rozdziale pracy.

## Ochrona konsumentów

Powszechnie uważa się użytkownika Internetu za słabszą stronę umów zawieranych za pośrednictwem sieci komputerowych. Ochrona konsumenta na tym polu to zasadnicza przesłanka poprawy bezpieczeństwa w Internecie oraz polepszenia poziomu świadczonych usług.

Na owe zagadnienia uwagę zwróciła Unia Europejska. Już w dyrektywie 85/577 z 20.12.1995 r. unormowano sprawę ochrony konsumentów przy umowach zawieranych poza miejscem prowadzenia handlu. Drugim aktem prawnym w tej materii jest dyrektywa Parlamentu i Rady Wspólnot Europejskich 97/7 z 20.05.1997 r. o ochronie konsumenta w umowach zawieranych na odległość (OJL 144/19 z 04.06.1997 r.)<sup>198</sup>.

Polski ustawodawca mający za zadanie harmonizację polskiego systemu prawnego z przepisami unijnymi wyszedł naprzeciw owym rozwiązaniom i dostosował nasze prawo do standardów Unii Europejskiej. Fundamentalne znaczenie ma tutaj ustawa z 02.03.2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz. U. nr 22 poz. 271).

Rozdział 2 tejże ustawy zatytułowany jest „Umowy zawierane na odległość”. Zawiera definicję umowy na odległość. Pozwolę sobie przytoczyć treść art. 6 ust. 1 ustawy. *Umowy zawierane na odległość z konsumentem bez jednoczesnej obecności obu stron przy wykorzystaniu środków porozumiewania się na odległość, w szczególności formularze zamówienia nie zaadresowanego lub zaadresowanego, listu seryjnego, reklamy prasowej z wydrukowanym formularzem zamówienia, katalogu, telefonu, radia, telewizji, automatycznego urządzenia wywołującego, wizjo fonu, wideo tekstu, poczty elektronicznej, telefaksu, są umowami na odległość jeżeli kontrahentem konsumenta jest przedsiębiorca, który w taki sposób zorganizował swoją działalność.*

Uwagę zwraca nie zamknięty katalog środków porozumiewania się na odległość oraz włączenie w ich zakres poczty elektronicznej. Z uwagi na szybki postęp technologiczny w sferze informatyki i telekomunikacji czyż nie lepiej byłoby ograniczyć się tylko do definicji przez postulaty. Wynika więc z przepisów ustawy, iż będzie ona miała zastosowanie także do umów zawieranych poprzez Internet.

O ile znaczenie umów zawieranych poprzez pozostałe środki porozumiewania się (z wyjątkiem telefonu) będzie maleć o tyle lawinowo przyrastać będzie wartość transakcji dokonywanych w sieciach komputerowych. Ustawa określa także definicję konsumenta- w przepisach nowelizacyjnych kodeks cywilny. Zakłada również szerokie uprawnienia konsumentów oraz nakłada na przedsiębiorcę szereg obowiązków. Spośród tych drugich najbardziej znaczące są:

- powiadomienie konsumenta o istotnych postanowieniach (art.9 ustawy),
- potwierdzenie, najpóźniej w momencie rozpoczęcia świadczenia, o większości informacji podanych pod zawartą umową.

Ważnym uprawnieniem po stronie konsumenta jest prawo odstąpienia od umowy, bez podania przyczyn, w terminie 10 dni od dnia wydania rzeczy. Sporną

---

<sup>198</sup> Szersze opracowanie tego tematu znajduje się w: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.100-105.

kwestię stanowi obowiązek poniesienia kosztów zwrotu zakupionych towarów<sup>199</sup>. Problemy w interpretacji stwarza art. 11 ust. 1- zakaz uiszczenia ceny za produkt przez konsumenta przed otrzymaniem świadczenia<sup>200</sup>.

Osobnym zagadnieniem jest ochrona konsumenta z uwagi na posługiwanie się przez przedsiębiorców wzorcami umów (regulaminami). Do umów *on line* – zawieranych w takiej formie - należy stosować przepisy dotyczące tzw. ogólnych warunków umów. Wzorce powinny być przedmiotem sprawdzenia czy skutecznie zostały wprowadzone do kontraktów z konsumentami oraz czy nie zawierają postanowień, które są niedopuszczalne<sup>201</sup>. Także tutaj dużą rolę odgrywa ustawa o ochronie niektórych praw konsumentów (...) z 02.03 2000 r.

Uważa się jednak, iż przepisy owej ustawy nadmiernie faworyzują konsumentów. Punkt ciężkości za bardzo przesunął się w ich stronę, co wiązać się może ze stwarzaniem trudności przedsiębiorcom funkcjonującym na rynku *e-commerce*.

## Dobra osobiste w Internecie

Związki Internetu z prawem cywilnym pojawiają się także w innych obszarach prawa cywilnego. Duże kontrowersje w nauce wzbudza naruszenie dóbr osobistych w sieci oraz ich ochrona w owym środowisku. Do naruszania takich dóbr osobistych jak wizerunek, nazwisko lub pseudonim, tajemnica korespondencji czy twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska często dochodzi w sieci Internet. Z uwagi na cechę sieci (anonimowość i skala działania) zjawiska te są niepokojące. Pojawiają się natomiast kłopoty dowodowe (trudność w określeniu kręgu odbiorców naruszenia, ustalenie czasu wejścia do systemu informatycznego, czy możliwość usunięcia czy sfalszowania informacji). Trudności stwarza także określenie rodzaju działania, które wkroczyło w cudze dobra osobiste (np. trudność taką stanowi przede wszystkim link- odnośnik<sup>202</sup>).

Kwestia dóbr osobistych i wiążących się z nimi danych osobowych zasługuje na szczegółowe przedstawienie. Niestety ramy pracy nie pozwalają mi na dokładniejsze omówienie tej materii.

## 4. Postępowanie cywilne

Zmiany przepisów prawa cywilnego materialnego oraz rozwój technologii spowodowały reakcje ustawodawcy w kwestii postępowania cywilnego. Reakcją tą było wprowadzenie do procesu cywilnego nowych uregulowań zawartych ustawie z dnia 24.05.2000 r. o zmianie ustawy Kodeks postępowania cywilnego, ustawy o zastawie rejestrowym i rejestrze zastawów (...) ( Dz.U.00.48.554).

---

<sup>199</sup> H. Fedorowicz, *Wycofać się łatwo, lecz trzeba wiedzieć kiedy*, Rzeczpospolita z dn. 04.01.2001 r.

<sup>200</sup> X. Konarski, *Prawo cywilne a Internet*, „Biznesnet” z 17.10.2000 r. , artykuł dostępny na stronie <http://www.biznesnet.pl/index.phtml?pg=ebiz&a=455>

<sup>201</sup> Ibidem.

<sup>202</sup> Zob. M. Domagalski, *Odsyłacze muszą zostać usunięte*, „Rzeczpospolita” z 02.03.2001.

Nie tylko nowe przepisy stanowią wyraz zmieniających się okoliczności. To także idące z postępowaniem technicznym orzecznictwo oraz doktryna naukowa.

## Pisma procesowe

Ważnym elementem czynności procesowych są pisma procesowe. Na mocy wspomnianej ustawy art. 125 k.p.c. uzyskał nowe brzmienie. Ustawodawca w §2 przewidział wnoszenie pism procesowych (wniosków i oświadczeń stron składanych poza rozprawą) na urzędowych formularzach oraz, co znamienne, na elektronicznych nośnikach informatycznych.<sup>203</sup>

Przepis ten i nowe rozwiązania są znaczące z uwagi na stałość i niezmiennosc procesu, który ze względu na swą materię posługuje się instytucjami sprawdzonymi <sup>204</sup>. Zapis taki wyraża więc stanowczą wolę ustawodawcy wprowadzenia szerokich zmian w procesie można je nawet uznać za rewolucyjne, gdyż przełamują one zasadę materialności pism procesowych (ich papierowej formy).<sup>205</sup>

Paragraf 4 art. 125 k.p.c. stanowi delegację ustawową dla Ministra Sprawiedliwości do wydania przepisów wykonawczych (w drodze rozporządzenia) określających szczegółowe zasady i termin wprowadzenia techniki informatycznej, warunki jakim powinny odpowiadać elektroniczne nośniki informatyczne, tryb odtwarzania danych na nich zawartych oraz sposób ich przechowywania i zabezpieczania. Pomimo, iż przepisy te weszły w życie 01.10.2000 roku aktu wykonawczego w tej materii nie ma. Przepis ów (art. 125 §2 k.p.c.) pozostaje więc przepisem martwym. Zauważyć wypada, iż stan wyposażenia sądów w sprzęt komputerowy jest niewystarczający na wprowadzenie tych rewolucyjnych zmian. Kolejny raz mamy do czynienia z przykładem, że za dobrą wolą nie podążają środki finansowe na realizację nowych rozwiązań.

Skutki niewniesienia pisma procesowego na elektronicznym nośniku informatycznym, gdy przepis szczególny to przewidywał, określa art.130<sup>1</sup> §1 (w związku z §2). Charakterystyczna jest tu sytuacja, w przypadku sprzeciwu od wyroku zaocznego, zarzutów od nakazu zapłaty lub sprzeciwu od nakazu zapłaty. W takich wypadkach, gdy nie zostały spełnione wszystkie przesłanki sąd odrzuca owe środki zaskarżenia (mają one charakter niedewolutywny).

## Doręczenia

Doręczenia są ważną czynnością procesową. Według A. Zielińskiego doniosłość prawidłowego doręczenia należy wiązać z jego skutkiem. Powstaje on w zasadzie z chwilą doręczenia. Właśnie w owej chwili zostaje spełniony cel doręczenia, czyli powiadomienie strony o treści dostarczonego pisma.<sup>206</sup>

---

<sup>203</sup> Tak jak w procesie karnym nie znajdujemy w przepisach prawa cywilnego definicji owych elektronicznych nośników informatycznych.

<sup>204</sup> *Kodeks postępowania cywilnego – komentarz tom I*, pod red. K. Piaseckiego, Warszawa 1999, s.482.

<sup>32</sup> Zakres spraw w których pisma procesowe należy wnosić na elektronicznych nośnikach informatycznych reguluje art. 187<sup>2</sup> k.p.c.

<sup>206</sup> A. Zieliński, *Postępowanie cywilne*, Warszawa 2000, s.80-81.

Mimo postępu technicznego ustawodawca nie zdecydował się na znaczące zmiany w dziedzinie doręczeń. Jedyłą nowością stanowi utworzenie na mocy art. 131 §1 k.p.c. sądowej służby doręczeniowej.<sup>207</sup>

Postępowanie cywilne niechętnie odchodzi od sprawdzonych rozwiązań jak już to podkreśliłem. W przypadku doręczeń z upływem czasu i w wyniku zwiększania się bezpieczeństwa elektronicznej korespondencji takie zmiany będą nieuniknione – znajdzie tu szerokie zastosowanie podpis elektroniczny w wersji kwalifikowanej w komunikacji pomiędzy jednostkami administracji rządowej, jednostkami samorządu terytorialnego czy sądami a obywatelami.<sup>208</sup>

Moim zdaniem zmiany w doręczeniach należy najpierw wprowadzić w kontaktach sądów z osobami prawnymi oraz z jednostkami organizacyjnymi nie posiadającymi osobowości prawnej (art.133 §2) oraz z przedsiębiorcami wpisanymi do rejestrów sądowych na podstawie odrębnych przepisów (art.133 §2a). Formę elektronicznych doręczeń należałoby umożliwić także w przypadku doręczania pism między adwokatami i radcami prawnymi w toku spraw (art. 132 §1 k.p.c.) .

Dzisiejsza technika informatyczna zapewnia wysoką jakość elektronicznych dokumentów, ich bezpieczeństwo, dokładne określenie czasu i miejsca ich odebrania, powiadomienie o ich odbiorze oraz znaczne obniżenie kosztów czynności procesowych, którymi są doręczenia. Sprawność, pewność i ekonomia procesowa powinny mieć tu duże znaczenie z uwagi na podstawowe zasady postępowania cywilnego.

## Dowody

Dowody stanowią źródło poznania przez sąd stanu faktycznego toczącego się przed nim procesu <sup>209</sup>. Jak kodeks postępowania cywilnego reguluje kwestię dowodów związanych z Internetem?

Nie ma nowych przepisów w tym ujęciu. Należy więc stosować już funkcjonujące z odpowiednią interpretacją. Według kodeksu dokumenty dzieli się na urzędowe (art. 244 k.p.c.) oraz prywatne (art.245). W momencie wejścia w życie ustawy o podpisie elektronicznym dokumenty w formie elektronicznej zostaną zrównane z dokumentami „papierowymi”. Tutaj także będzie można wyodrębnić dokumenty urzędowe oraz prywatne<sup>210</sup>. Do dokumentów elektronicznych będą miały zastosowanie przepisy dotychczasowe o dokumentach– art. 244- 257 k.p.c.

Rozważania nad uznaniem za dowód wydruku komputerowego zejda więc na dalszy plan<sup>211</sup>. Wszystko, jak widzimy, w tym przedmiocie zależy od ustawy o podpisie elektronicznym.

Szeroki zakres zastosowania w stosunku do Internetu będzie miał art. 309 k.p.c. – inne środki dowodowe<sup>212</sup>. Przepis ten umożliwi sądowi przeprowadzenie

<sup>207</sup> Paragraf 3 art. 131 k.p.c. określa delegację dla Ministra Sprawiedliwości do utworzenia sądowej służby doręczeniowej w drodze rozporządzenia.

<sup>208</sup> Czas i miejsca dokonania doręczenia a co za tym idzie i całą materią elektronicznych doręczeń zajmuje się modelowa ustawa UNCITRAL w art.14-15.

<sup>209</sup> A. Zieliński, *Postępowanie cywilne*, op. cit., s.113.

<sup>210</sup> Poselski projekt ustawy o podpisie elektronicznym zakłada, iż dokumenty będą sygnowane albo podpisem zwykłym albo kwalifikowanym – w obrocie z jednostkami administracji państwowej.

<sup>211</sup> K. Knoppek, *Wydruk komputerowy jako dowód w procesie cywilnym*, „Państwo i Prawo” 1993/2/54.

<sup>212</sup> Na przykład przeprowadzenie dowodu z zawartości strony WWW, na której umieszczono materiały godzące w czyjeś dobra osobiste.

dowodu z użyciem bardzo nowoczesnych technologii, choć jak wiemy środek dowodowy powinien posiadać określone cechy.

W stosunku do Internetu i elektronicznych nośników informacji zastosowanie znajdzie art. 308 k.p.c. Według §2 tegoż artykułu dowody takie sąd przeprowadza stosując odpowiednio przepisy o dowodzie z oględzin oraz z dokumentów.

Do momentu wejścia w życie ustawy o podpisie elektronicznym wydawałoby się, że w polskim procesie cywilnym nie będzie możliwe uznanie dokumentu elektronicznego za dowód. Sytuację tą zmienia całkowicie art. 1138 k.p.c., który stanowi, iż zagraniczne dokumenty urzędowe posiadają moc dowodową na równi z polskimi dokumentami urzędowymi. Internet ma globalny zasięg a ilość krajów stosujących podpis elektroniczny systematycznie rośnie.<sup>213</sup>

Widzimy więc, że już teraz polski ustawodawca dopuścił dokumenty elektroniczne do postępowania cywilnego, choć jak można się domyślać stało się to raczej nieświadomie.

W związku ze zwiększającymi się obrotami handlowymi w sieci oraz globalnym oddziaływaniem Internetu należy zauważyć, iż coraz większego znaczenia będą nabierać przepisy prawa międzynarodowego prywatnego – przede wszystkim rozdziały IX-XI ustawy prawo międzynarodowe prywatne z dnia 12.11.1965 r. Kwestię dotyczącą podpisu elektronicznego oraz uznania przez polskie sądy elektronicznych dokumentów przedstawiłem powyżej.

Na pierwszy plan wysuwają się uregulowania umów zawieranych poprzez sieć. W tym zakresie strony mogą poddać swe stosunki wybranemu przez siebie prawu, jeżeli pozostaje ono w związku ze zobowiązaniem (art.25 §1 ustawy prawo międzynarodowe prywatne). Gdy strony takiego wyboru nie dokonają należy stosować przepisy prawa, w którym strony w chwili zawarcia umowy mają siedzibę lub miejsce zamieszkania. Sytuację, gdy strony takiej wspólnej siedziby lub miejsca zamieszkania nie mają stosuje się przepisy art. 27 ustawy.

Pamiętajmy także, iż zawieranie umów sprzedaży reguluje Konwencja Wiedeńska z 1980 r. O kontraktach międzynarodowej sprzedaży towarów.<sup>214</sup>

Zakres mej pracy oraz złożony charakter problemów Internetu w prawie cywilnym (materialnym i procesowym) nie pozwoliły mi niestety na głęboką analizę ich wszystkich. Często musiałem pozostać przy krótkim zwróceniu uwagi na ciekawe zagadnienia. Sam tylko podpis elektroniczny mógłby stać się przedmiotem osobnej pracy naukowej. Przekrój przez najważniejsze dziedziny pozwala dojść do pewnych wniosków. Są one jednoznaczne.

Prawo nie nadąża za zmianami w życiu codziennym. Technologia, która wyprzedza prawne rozwiązania w określony sposób wywiera nacisk na ustawodawcę, aby reakcja na zachowania w obrocie handlowym następowała sprawniej i szybciej. Przejawem tych zmian są projekty ustawy (poselski i rządowy) o podpisie elektronicznym oraz w ustawie o księgach wieczystych i hipotece. Wraz z rozwojem i udoskonalaniem sposobu przekazywania

---

<sup>213</sup> I. Sitnicki, M. Srebrny, *Jak podpisuje się świat*, „Rzeczpospolita” z 09.02.2001 r.

<sup>214</sup> Szerzej na ów temat: A. Kocot, *Zawieranie umów sprzedaży według Konwencji Wiedeńskiej*, op. cit.

wiadomości- dokumentów (poczta elektroniczna) możemy oczekiwać zmian w systemie doręczeń w postępowaniu cywilnym.<sup>215</sup>

Postęp sprawia, iż nie możemy stanowczo opierać się na dotychczasowych założeniach prawa cywilnego. Prawo powinno dostosowywać się do zmieniających się realiów i przykłady tego znajdujemy w całym prawie cywilnym.

### 3. Prawo autorskie

#### Przedmiot i podmiot prawa autorskiego

Znaczenia prawa autorskiego w Internecie nie sposób nie docenić. Wiele zachodzących w sieci zjawisk próbuje się tłumaczyć i rozwiązywać za pomocą prawa autorskiego. Jednak ów dział prawa prywatnego przeobraża się pod wpływem Internetu.

Zasadniczym zadaniem w ramach rozważań o prawie autorskim jest zdefiniowanie przedmiotu prawa. Artykuł 1 ustawy o prawie autorskim i prawach pokrewnych (Dz.U.00.80.904) określa definicję przedmiotu prawa autorskiego. Jest nim utwór- niematerialne dobro prawne, będące każdym przejawem działalności twórczej o indywidualnym charakterze, które zostało ustalone w jakiegokolwiek postaci, bez względu na wartość, przeznaczenie czy sposób wyrażenia. Technika informatyczna sprawia, iż stały się dostępne nowe rodzajowo rezultaty pracy ludzkiej, które aspirują do kategorii utworów objętych ochroną prawa autorskiego<sup>216</sup>.

Oprócz nowych rodzajów utworów pojawiły się także „tradycyjne utwory” przystosowane do funkcjonowania (zaistnienia) w sieciach komputerowych. Zjawisko to nazywamy digitalizacją, czyli ustalenie utworu w postaci zapisu cyfrowego. Dzieło takie zapisane w systemie 0-1 nie zyskuje cech decydujących o przyznaniu mu ochrony prawa autorskiego. Nie można również zastosować tego rozwiązania w przypadku utraty tych praw tylko dzięki digitalizacji.

Digitalizacja utworu nie może być także traktowana jako opracowanie (utwór zależny), gdyż opracowanie jest chronione przez prawo autorskie lecz jest to skutkiem dodania do przejętych cech twórczych oryginalnych własnych i nowych cech. Jak podkreślają J. Barta i R. Markiewicz sytuacja taka nie występuje przy digitalizacji, choć samo jej wykonanie wymaga zastosowania zdobytej wiedzy i umiejętności<sup>217</sup>. Jak sugerują wymienieni autorzy rezultat procesu digitalizacji uzyska status przedmiotu objętego ochroną w ramach praw pokrewnych. Ów postulat nie ma jednak podstawy w przepisach żadnego państwa.

Zachwianiu uległa, poprzez ingerencję informatyki w sferę prawa autorskiego, zasada nakazująca chronić niezależnie od całości dzieła także jego części (o ile wykazują stopień oryginalności). Sam proces digitalizacji polega na

---

<sup>215</sup> Technika informatyczna już wkrótce może spowodować iż same rozprawy będą odbywać się w sieci. Wydaje się to odległą przyszłością a jednak w Australii prace nad takim projektem trwają.

A. Creed, *Australian state may bring courts procedures online*, “Newsbytes”, 04.01.2001 r.  
<http://www.newsbytes.com/news/01/160072.html>

<sup>216</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.112.

<sup>217</sup> Ibidem, s.113.

rozbiciu na elementarne składniki utworu i przetwarzanie go na język danego programu komputerowego. Jednakowy cyfrowy zapis zmusza do pytania o sens utrzymywania w obrębie ustaw wyraźnej kategoryzacji utworów. Czy zachowują one swe znaczenie (szczególne rozwiązania), a przynajmniej pełne dotychczasowe znaczenie, w erze digitalizacji wszelkich efektów pracy twórczej, zwłaszcza gdy dochodzić do tego będzie w coraz większym stopniu wspólna płaszczyzna eksploatacji (eksploatacja w sieciach komputerowych)? - pytają autorzy pracy *Internet a prawo*<sup>218</sup>.

W sieci pojawiają się nowe formy utworów. Produkty multimedialne łączą w sobie elementy różnych dziedzin sztuki i różne środki wyrazu (słowo, obraz, muzykę, animację). Zostały jednak sprowadzone do jednorodnego zapisu cyfrowego. Produkty te udostępniane są zarówno w Internecie jak i poza nim (np. płyty CD).

Sposób powstawania dzieł multimedialnych (łączenie wielu fragmentów w jedną całość), ich natura i postać pozwalają zakwalifikować je w zakres ochrony praw autorskich (a nie pokrewnych). Takie stanowisko stwarza pytanie o kategoryzację tego rodzaju dzieł.

W literaturze zdania są podzielone. Przeważa pogląd, iż należy je rozpatrywać w odniesieniu do poszczególnych przypadków (*casu ad casum*). Problem kwalifikacji danego produktu multimedialnego ma praktyczny charakter, gdyż ustawa o prawie autorskim przewiduje szczególną regulację dla utworów filmowych, audiowizualnych, baz danych czy programów komputerowych. Duże problemy stwarza problematyka ochrony dzieł multimedialnych<sup>219</sup>.

Stosunkowo nową kategorią utworów są programy komputerowe. Samo funkcjonowanie sieci opiera się właśnie na ich działaniu. Na podstawie przepisów szczególnych w ustawie o prawie autorskim (art.74-77) zostały one objęte ochroną prawa autorskiego. Jest więc to regulacja szczególna wykazująca znaczne różnice w stosunku do ogólnej, dotyczącej innych kategorii dzieł.

Istotnym *novum* przepisu art. 3 ustawy jest uwzględnienie w nim baz danych jako odrębnego przedmiotu ochrony<sup>220</sup>. Pojawił się pogląd, iż sam Internet jako całość jest jedną wielką bazą danych i na tej podstawie powinien być objęty ochroną prawa autorskiego. Z owym zdaniem należy się nie zgodzić, gdyż kto wtedy byłby tutaj podmiotem prawa? Zarysowują się także kwestie dostępu do źródeł informacji, wolności wypowiedzi i komunikowania się. W Polsce ochroną objęte są te bazy danych, które wykazują „twórczy” charakter. Może się on przejawiać w układzie, zestawieniu elementów składowych czy też ich doborze. Problem baz danych i ich ochrony jest znaczący z uwagi na rozmiary informacji gromadzonych i przesyłanych w Internecie. Zakres i doniosłość tej tematyki sprawiają, iż wymaga ona osobnego omówienia w niniejszej pracy<sup>221</sup>.

Internet stworzył w swym zakresie charakterystyczne dla siebie „dzieła i utwory”. Są nimi strony WWW (będzie tu mowa przede wszystkim o tzw. *home pages*), menu, ikony, linki- odsyłacze. Jak traktować domowe strony WWW, które poprzez układ powiązań przenoszą nas do kolejnych „pokoi”, „plansz”? Czy mają

---

<sup>218</sup> Ibidem.

<sup>219</sup> Szerzej na ów temat: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.116-117.

<sup>220</sup> J. Barta, R. Markiewicz, *Komentarz do ustawy o prawie autorskim i prawach pokrewnych*, Warszawa 1995.

<sup>221</sup> Patrz: Rozdział V *Adresy internetowe, bazy danych i ich ochrona*.

one charakter przejawu o twórczej działalności, indywidualnym charakterze? Czy zatem są według przepisów ustawy o prawie autorskim przedmiotem ochrony? Posługiwanie się oryginalnymi elementami graficznymi, charakterystyczną typografią czy układem- rozmieszczeniem powoduje, iż wiele stron ma twórczy charakter. Jak więc oceniać je z punktu widzenia prawa autorskiego? A jeśli się zaakceptuje, iż są one objęte ochroną to z jaką kategorią dzieła mamy do czynienia?

Orzecznictwo w Niemczech i USA traktuje strony WWW (*home pages*) jak naukowe czy techniczne prezentacje<sup>222</sup>. Podobny problem dotyczy menu i ikon na prezentowanych stronach. Określa się je jako metodę obsługi programu/stron co wiąże się z wyjęciem ich spod ochrony prawa autorskiego. Analogicznie rozwiązania możemy zastosować w stosunku do odesłań - tzw. linków umieszczanych na stronach WWW (choć chociaż tzw. hiperlinki funkcjonują także pomiędzy stronami WWW). Ocena owych odesłań jest jednoznaczna. Nie mają one cech oryginalnych, nie są twórcze i przez to nie stanowią przedmiotu ochrony w świetle przepisów prawa autorskiego<sup>223</sup>.

Dziś technika komputerowa pozwala uzyskać taką jakość animacji, która dla zwykłego widza nie różni się niczym od normalnej gry aktorskiej. Postęp w tej dziedzinie sprawił, że komputery uczyniły animację tańszą, o lepszej jakości oraz szybszą od tradycyjnych technik stosowanych dotąd. Skanując bowiem dokumentację ikonograficzną określonej postaci możemy uzyskać materiał informatyczny pozwalający ożywić wizerunek tej osoby na ekranie komputera (czy też telewizora w efekcie końcowym). Czy taka „stworzona postać” może korzystać z ochrony w oderwaniu od programu, który ją stworzył?<sup>224</sup> Ugruntował się w tej dziedzinie pogląd, iż takowe wirtualne postacie i ich plastyczne wizerunki podlegają na ogólnych zasadach ochronie płynącej z przepisów prawa autorskiego. Żadnej osobie nie przysługują prawa autorskie do jej wyglądu<sup>225</sup>.

W takim jednak przypadku (wirtualnych wizerunków osób żyjących czy nieżyjących) pojawia się ponadto kwestia ochrony dóbr osobistych - takich jak prawo do wizerunku, prawa związane z kultem osoby zmarłej.

Nowe rodzaje dóbr, które funkcjonują w sieci stwarzają problemy w zakresie ustalenia podmiotu prawa autorskiego. Idealizujący przepis art. 8 ustęp 1 ustawy o prawie autorskim i prawach pokrewnych określa podmiot prawa autorskiego. Jest nim twórca o ile ustawa nie stanowi inaczej. Nowe utwory w Internecie często wymagają dużych nakładów, środków technicznych, kapitału. Coraz częściej tym zadaniom podołać mogą tylko duże firmy czy instytuty badawcze. Wymaga to także międzynarodowej współpracy, która dotyczy całych zespołów naukowych i eksperckich. Późniejsza eksploatacja i dysponowanie prawami osobistymi do utworów wymagałoby uzyskania zezwolenia wielu autorów dzieła.

Bezwzględna zasada określająca jako podmiot prawa twórcę utworu doznaje jednak w tym punkcie ograniczenia. Jest ono konieczne z uwagi na ułatwienie obrotu handlowego i klarowną sytuację prawną określonego utworu.

---

<sup>222</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.121.

<sup>223</sup> Ibidem, s.122.

<sup>224</sup> Pamiętajmy, że mogą być to wizerunki osób fantastycznych, żyjących jak i już umarłych.

<sup>225</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.123-124.

Przyjęcie takiego założenia, iż prawa autorskie przysługują producentowi jest takim właśnie ułatwieniem. Ponadto przepisy szczególne już wprowadziły tego rodzaju rozwiązania (np. w przypadku programów komputerowych). Samo rozumienie terminu twórcy jest w ustawie nie do końca jasne<sup>226</sup>. Jak podkreślają ciż sami autorzy w pracy *Internet a prawo* (strona 125) powoli, lecz stale, rośnie też na terenie prawa autorskiego liczba przypadków, w których prawo to „odsuwa się” od autora w kierunku producenta. Kolejny problem w zakresie podmiotu prawa autorskiego to problem współautorstwa. Jak oceniać luźne formy współpracy pomiędzy użytkownikami Internetu na polu tworzenia danych produktów? Dotyczy owe pytanie, przede wszystkim funkcjonowania BBS (*Bulletin Board Systems*), poprzez które osoby udostępniają sobie nawzajem własne materiały niekiedy o cechach twórczych, oraz w połączeniu z cudzymi materiałami.

Kolejny dylemat pojawia się przy ustaleniu autorstwa w przypadku posługiwania się oprogramowaniem. Czy autor oprogramowania będzie także współautorem stworzonego, dzięki właśnie temu programowi, innego dzieła osoby trzeciej? Wydaje się, jak to już wcześniej zasygnalizowałem, iż program jest tu jedynie narzędziem i nie będzie dawał swemu twórcy podstawy do podobnych roszczeń.

W sieci wiele utworów jest anonimowych - wiąże się to z samym charakterem Internetu. Sytuację tą reguluje art. 8 ustawy o prawie autorskim, zastępując tu anonimowego twórcę producentem, wydawcą czy organizacją zbiorowego zarządu prawami autorskimi. Lecz kogo w takich wypadkach uznać za wydawcę czy producenta? Czy ma być nim operator systemu, właściciel serwera, firma telekomunikacyjna czy może jeszcze ktoś inny?

## Eksploatacja i wprowadzenie utworu do sieci

Znaczącym problemem ze względu na swe konsekwencje prawne jest zagadnienie wprowadzenia utworu do sieci komputerowej. W momencie wprowadzenia dzieła do Internetu staje się on dostępny na całym świecie bez względu na czas i miejsce. Jak określają to J. Barta i R. Markiewicz (*Internet a prawo*, s.128) staje się on potencjalnie dostępny dla wielu użytkowników sieci komputerowej. Samo udostępnienie utworu w sieci jest czynem relewantnym z punktu widzenia prawa autorskiego, jako wkroczenie w prawa majątkowe (eksploatacyjne, obejmujące korzystanie z utworu i rozporządzanie nim we wszystkich polach eksploatacji- art. 17 prawa autorskiego).

Wprowadzenie dzieła do Internetu wiąże się z trzema zasadniczymi skutkami prawnymi owego postępowania. Czy taki utwór należy uznać za:

1. rozpowszechniony,
2. opublikowany,
3. wprowadzony do obrotu?

**Ad.1.** Zawarta w ustawie o prawie autorskim i prawach pokrewnych (art.. 6 pkt 3) definicja utworu rozpowszechnionego wskazuje, iż jest nim „utwór, który za

---

<sup>226</sup> Różne określenia terminu twórca znajdziemy w: J. Barta, R. Markiewicz, *Komentarz do ustawy o prawie autorskim i prawach pokrewnych*, op. cit., s.100-101.

zezwoleń twórcy został udostępniony publicznie”<sup>227</sup>. Pominę tu kwestię związaną z osobą (podmiotem), która wprowadza utwór do sieci, gdyż już wcześniej zaznaczyłem jak różnie ustawodawca definiuje twórcę utworu.

Zastanówmy się nad kolejną przesłanką definicji – publicznym udostępnieniem. W Internecie są miejsca (strony WWW) dostępne tak publicznie jak i o ograniczonym dostępie. Z uwagi na definicję rozpowszechniania przychylić się należy do twierdzenia, aby można było wprowadzenie do sieci uważać za rozpowszechnianie musi ono nastąpić w miejscach dostępnych publicznie. Nie ma tu znaczenia, jak i ile osób dotrze do danego utworu czy też gdzie one się będą znajdować. Podkreśla się w nauce, iż przepisy dotyczące publicznego rozpowszechniania (komunikacji publicznej) stosować należy w drodze analogii do eksploatacji dzieł w międzynarodowych sieciach komputerowych, ze względu na to, iż „tradycyjne” komunikowanie publiczne oraz dostęp w sieci do utworu na żądanie różnią się w zasadzie tylko pod kątem technicznym<sup>228</sup>.

W przypadku wprowadzenia utworu do sieci w ramach komunikacji indywidualnej (*e-mail*, poczta elektroniczna) nie możemy uznać stosownego zachowania za rozpowszechnianie. Komunikacja taka występuje także w handlu elektronicznym – EDI. Indywidualnego charakteru komunikacji nie odbiera to, iż na drodze między nadawcą a odbiorcą informacja przepływa przez urządzenia będące w dyspozycji osoby trzeciej (dostarczyciela usług sieciowych)<sup>229</sup>.

Przy uznaniu wprowadzenia do sieci utworu za rozpowszechnianie pojawiają się jak widzimy znaczące problemy. Uznać jednak należy, iż w świetle polskiego prawa autorskiego takie działanie jest rozpowszechnianiem<sup>230</sup>.

**Ad.2.** Utworem opublikowanym jest utwór, który za zezwoleniem twórcy został zwielokrotniony i którego egzemplarze zostały udostępnione publicznie-art. 6 pkt 1 ustawy o prawie autorskim

Nie chodzi więc tutaj, jak możemy zauważyć, o publiczne udostępnienie samego utworu lecz o udostępnienie jego egzemplarzy. Można mieć wątpliwości co do uznania za publikację wprowadzenia elektronicznego utworu do sieci. Trudno wykazać, iż eksploatacja następuje poprzez udostępnianie egzemplarzy w Internecie. Mimo wszystko w przypadku tym należy rozpatrywać te kwestie *ad casum*. Zmiana podejścia jednak może nastąpić albo poprzez zmianę definicji

---

<sup>227</sup> W literaturze można spotkać zdania, iż nie należy stosować tej definicji do sieci komputerowych, gdyż w momencie tworzenia przepisów ustawy nie były one brane pod uwagę. Podobną wykładnię można zastosować przy artykule 31 ust.4 ustawy, który sprzeciwia się rozszerzeniu stosowania umów autorskich na pola eksploatacji nie znane w chwili ich zawarcia. Jednak tak podana wykładnia byłaby błędna, ponieważ brak jest odniesienia do korzystania z utworów w Internecie (czy szerzej przy zastosowaniu nowoczesnych technik) nie ma dużego znaczenia przy generalnej definicji zawartej w art.6 pkt 3.

<sup>228</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.129 za Th. Hoeren, *The Green Paper on Copyright and Related Rights in the Information Society*, EPIR 1995/10, s.514.

<sup>229</sup> W nowej konwencji WIPO dotyczącej praw autorskich przyjęto nową definicję rozpowszechniania. Stwierdza ona, iż rozpowszechnianie jest tego rodzaju publicznym udostępnieniem utworu drogą bezprzewodową lub przewodową, gdy podejmowane są indywidualne decyzje odnośnie miejsca lub czasu odbioru. Nie zgodzono się na wyjęcie spod ochrony utworów pochodzących z krajów spoza konwencji.

<sup>230</sup> Pojawiają się jeszcze dwa zagadnienia- pierwszym z nich jest stwierdzenie, iż choć utwór został wprowadzony do sieci to faktycznie mógł zostać nie odebrany (publiczna percepcja). Drugim z nich jest wprowadzenie utworu do sieci zamkniętej (Intranetu). W obu tych kwestiach można zastosować zasady rządzące w przypadku „zwykłych” utworów (program radiowy, wykonywanie dzieł podczas zamkniętych imprez).

„publikacji”, albo odmienne od dotychczasowego rozumienie terminu „egzemplarz”<sup>231</sup>

**Ad.3.** Trudno także uważać wprowadzenie i eksploatację utworu w sieci komputerowej jako wprowadzenie do obrotu. Sama ta instytucja zakłada przeniesienie własności egzemplarza utworu. Przy eksploatacji utworu w sieciach komputerowych można mówić zaś o zwielokrotnieniu lecz nie ma podstaw, aby uważać je za obrót egzemplarzami. I choć często podkreśla się, iż sam obrót wiąże się z okolicznościami ekonomicznymi (np. utrata kontroli ze strony uprawnionego nad egzemplarzem książki od chwili sprzedaży) to ogranicza się to tylko do momentu decydowania przez wydawcę czy autora o danym obrocie takimi egzemplarzami. Jest to tak zwana instytucja wyczerpania prawa.

Podobne problemy pojawiają się przy eksploatacji utworu w sieci i poprzez sieć. Nowe sposoby korzystania z dzieł wymykają się często z ram starych przepisów. Ogromna ilość owych dzieł rodzi poważne konsekwencje. Skłaniać to może do zmiany znaczenia części stosowanych dziś definicji, pojęć tak aby mogły one skuteczniej funkcjonować w nowym środowisku jakim jest Internet.

Istotą zagadnienia jest usunięcie wątpliwości w jakim stopniu korzystanie z utworów poprzez Internet powinno być objęte treścią prawa autorskiego, gdy chodzi o decydowanie o cyfrowy przekaz utworu i jego odbiór przez użytkownika sieci.

Na treść prawa autorskiego składa się wiele samodzielnych „częstkowych” praw odpowiedzialności wyodrębnionych form eksploatacji (np. zwielokrotnianie utworu, jego nadawanie, wyświetlanie itd.)<sup>232</sup>. Są to :

1. Skanowanie i digitalizacja, wydruk komputerowy. Nie stwarzają one poważniejszych problemów prawnych. Same procesy skanowania i digitalizacji (*input*) oraz wydruk komputerowy (*output*) należy uznać za zwielokrotnienie w rozumieniu przepisów prawa autorskiego.

2. *Uploading* na własnym serwerze (komputerze). Nagranie utworu na własnym komputerze (w celu późniejszego oferowania go dalszym użytkownikom) danego utworu również należy zakwalifikować jako zwielokrotnienie określoną techniką. Z uwagi na problemy ze zdefiniowaniem egzemplarza nie będziemy mogli ująć tego typu zachowania jako wprowadzenie do obrotu. Samo wczytanie i cyfrowe zapisanie jest jednak kwestionowane. Dotyczy to kwestii niewystępowania materialnej kopii, utwór sam w sobie jest „niepoznawalny”. Prawo autorskie, mimo tego, jest zorientowane na niematerialne dobra intelektualne a nie na przedmiot fizyczny. Gdy poznawalność utworu zależy od posłużenia się odpowiednim narzędziem nie ma to znaczenia przy wyjęciu dzieła spoza zakresu ochrony prawa autorskiego.

Polskie prawo autorskie wyodrębnia „zwielokrotnienie określoną techniką”, „utrwalenie” oraz „wprowadzenie do pamięci komputera”. Jest to jednak mniej znaczące zagadnienie od odpowiedzi na pytanie czy rezultat procesu *uploading* można uznać za „egzemplarz utworu”. Przepisy ustawy w niektórych warunkach zezwalają na sporządzanie egzemplarzy chronionych utworów w ramach licencji ustawowych. Zauważmy, iż analiza przepisów ustawy posługujących się pojęciem „egzemplarz” prowadzi do uznania go za materialny nośnik utworu zdolny do

<sup>231</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.131-132.

<sup>232</sup> Ibidem, s.133.

samodzielnej cyrkulacji i stanowiący odrębne dobro (rzecz) w rozumieniu prawa<sup>233</sup>. Takim egzemplarzem może być dyskietka czy krążek CD-ROM. W kwestii podmiotu dokonującego aktu zwielokrotnienia utworu należy zająć stanowisko, iż jest nim ten kto dokonuje przegrania utworu<sup>234</sup>. Nie ma znaczenia natomiast kto jest dysponentem medium, z którego dokonano procesu *uploading* (choć w materii tej zdania są podzielone).

3. *Uploading* na obcym serwerze (komputerze). Za zwielokrotnienie uznaje się także przekazanie na cudzy serwer utworu poprzez tzw. *chat room'y* czy BBS (*Bulletin Board System*). Tu również nie możemy mówić o wprowadzeniu do obrotu. Samo przesłanie dzieła nie ma charakteru nadania. Jest tu bowiem charakterystyczne to, iż nadany utwór dociera bezpośrednio do odbiorcy.

4. *Downloading, browsing* (przeglądanie). Proces *download* jeśli tylko prowadzi do trwałego zapisania utworu oferowanego w ogólnie dostępnej bazie danych powinien być oceniany podobnie jak *uploading*. Dużym problemem jest uznanie przeglądania, (*browsing*) na ekranie monitora ściągniętych materiałów, za zwielokrotnienie utworu. Zapisanie następuje w pamięci operacyjnej (RAM).<sup>235</sup>

5. Przesyłanie danych w sieciach- komunikacja *on - demand*. Internet to przede wszystkim przesyłanie danych (w tym także materiałów objętych ochroną). Gdy mowa o przekazywaniu danych samoczynnie nasuwa się podobieństwo z postacią eksploatacji, którą jest nadawanie. Aby można jednak było mówić o nadawaniu konieczne jest to, aby dochodziło do publicznego udostępniania utworów drogą przewodową lub bezprzewodową. „Publiczny odbiór” skupia na sobie szczególną uwagę. Znajdziemy w tym wypadku dużo cech wspólnych z telewizyjnym czy radiowym przekazywaniem. Nie można komunikacji *on demand* (na życzenie) traktować jako „nadawania” w rozumieniu prawa autorskiego. Nie należy także traktować jej jako wprowadzenia do obrotu. Następuje zaś zwielokrotnienie materiałów, na które zgłoszono zapotrzebowanie. Niektórzy postrzegają oferowanie takich materiałów jako nowe (nienazwane) pole eksploatacyjne objęte treścią prawa autorskiego<sup>236</sup>.

6. Komunikacja indywidualna, poczta elektroniczna. Taka forma komunikacji nie stanowi rozpowszechniania utworów. Nie występuje tu bowiem „publiczny charakter”. Przy poczcie elektronicznej występują dwa skrajne poglądy. Pierwszy z nich stanowi, iż mamy tu do czynienia z czynnością nieistotną z punktu widzenia prawa autorskiego. Nie można przecież zajmować się wszystkimi czynnościami, które w jakikolwiek sposób dotyczą utworów. Drugi pogląd zakłada zwielokrotnienie utworu, gdy w rzeczywistości utwór nie tylko „wędruje” od nadawcy do odbiorcy lecz także gdy u odbiorcy powstaje kopia utworu- jest on zapisany po stronie nadawcy. Mieści się to jednak w ramach dozwolonego użytku prywatnego. Zatem nie można posłużyć się to roszczeniami zakazowymi wprowadzonymi z prawa autorskiego. Do naruszenia prawa autorskiego dochodzi wtedy gdy przesyłanie pocztą elektroniczną materiałów nie mieści się w granicach wytyczonych ustawowym dozwolonym użytkowaniem

---

<sup>233</sup> Ibidem, s. 135-136.

<sup>234</sup> Wiazać się to będzie z ewentualną odpowiedzialnością z tytułu naruszenia prawa.

<sup>235</sup> Szersze opracowanie tego tematu znajduje się w: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.136-141.

<sup>236</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.142 oraz P. Kościelniak, *Filmy na życzenie*, „Rzeczpospolita” z dnia 28.12.2000 r.

(osobistym czy publicznym). Rozpowszechnianie za pomocą poczty elektronicznej będzie miało miejsce jedynie wtedy, gdy mamy do czynienia z listą adresatów na tyle obszerną, iż nie będzie możliwe przyjęcie komunikowania prywatnego<sup>237</sup>.

7. Przesyłanie aktualizacji. Popularną usługą w sieci jest dokonywanie prenumeraty wybranych przez użytkownika aktualizacji, stron WWW, informacji, zbiorów albo artykułów na wskazany temat. Określa się to mianem *Digital Bindery*. Sam problem cyfrowej prenumeraty zbliża się do zagadnienia zwielokrotniania i nadawania. Cechy podobne możemy także znaleźć z *caching'iem*, który omówię w punkcie 9.

8. Łączenie z cudzymi stronami WWW. Bardzo kontrowersyjne jest łączenie się z innymi stronami w sieci World Wide Web. Czy samo bezpośrednie odwołanie się do innych stron (link) przez dostawcę usługi lub dysponenta strony stanowi naruszenie prawa autorskiego? Czy odesłanie do cudzej strony jest dozwolone? Odpowiedź na pierwsze pytanie wydaje się być jasna. Nie stanowi naruszenia praw autorskich odesłanie do innych stron WWW. To nie dostawca czy dysponent stron lecz końcowy użytkownik łączy się ze wskazaną linkiem stroną. Pojawia się tu jednak problem nieuczciwej konkurencji oraz posługiwania się cudzymi znakami towarowymi (są nimi przecież adresy WWW).<sup>238</sup>

9. *Caching*. Na wstępie kilka słów o samym procesie *caching'u*. Chodzi tu o dokonywanie automatycznego zapisywania w pamięci komputera (na tzw. *cache* serwer) adresów stron WWW (a co za tym idzie także i utworów w postaci tzw. *cookies*<sup>239</sup>). Ma to zwiększyć efektywność i szybkość transferu danych w przypadku trudności w wywoływaniu materiału zlokalizowanego na odległym komputerze (w rzeczywistości chodzi tu o jakość łącza i szybkość transferu danych). Dominuje pogląd, że działania takie objęte są dorozumianym zezwoleniem (licencją) ze strony wprowadzającego utwór do Internetu<sup>240</sup>.

Cóż jednak w przypadku uczynienia zakazu dokonywania *caching'u* przez dostawcę zawartości w sieci? Taki zakaz należy uznać w stosunku do eksploatacji objętej dozwolonym użytkowaniem prywatnym czy publicznym. *Caching* pokrywa się także z tymczasowym utrwaleniem w pamięci RAM. Takie zachowanie wkracza w monopol autorski. Na gruncie *caching'u* pojawiają się różne koncepcje mające rozwiązać problem zapisu przeglądanych materiałów na serwerze. Jedną z nich jest ustanowienie nieodwołalnej licencji w stosunku do utworu wprowadzonego do sieci. Innym – objęcie ustawowym dozwolonym użytkowaniem publicznym wszelkich dzieł znajdujących się w Internecie.

10. Telewizja interaktywna, Internet a technologie cyfrowe. Internet przebojem wkracza także i do telewizji. Nie tylko stanowi on jednak konkurencję

---

<sup>237</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.144.

<sup>238</sup> Ciekawy *casus* przytaczają autorzy *Internet a prawo*, s. 145-148.

<sup>239</sup> „Przed okręgowym sądem w nowym Jorku toczy się kilka spraw przeciwko praktyce używania przez DoubleClick – firmy zajmującej się reklamami w Sieci – technologii cookies. Wedle powodów – używanie technologii narusza szereg amerykańskich ustaw: the Electronic Privacy Act, the Wiretap Act oraz the Computer Fraud and Abuse Act. Cookies to niewielkie pliki komputerowe wysyłane przez serwer www komputerowi osoby odwiedzającej strony www, które zbierają dane o ruchu tego użytkownika w Sieci. Wedle powodów DoubleClick używa tej technologii w sposób naruszający prawo do prywatności użytkowników” – informacja zaczerpnięta za strony WWW: [http://www.vagla.pl/prawo\\_008.htm](http://www.vagla.pl/prawo_008.htm)

<sup>240</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.148.

wobec niej lecz może uzupełniać jej program oraz stwarzać nowe usługi<sup>241</sup>. W przypadku *near-video-on demand* ten sam program jest przekazywany na wielu równoległych kanałach w określonych odstępach czasu (np. co 5 minut). Podobnie jak w *pay-per-view* widz płaci za pojedyncze emisje, które nie występują w porządku zaplanowanym lecz są powtarzane periodycznie. W ramach *video-on demand* widz ma możliwość przeglądania katalogu z programem (filmami) wraz z krótkimi sekwencjami oraz po dokonaniu wyboru i zapłaty określonej kwoty może oglądać w dogodnym dla siebie terminie dany program. Występuje więc tu przekaz danych na masową skalę, do oznaczonych indywidualnie odbiorców. Będziemy mogli tu analogicznie zastosować rozwiązania dotyczące przekazu danych. Jednak tak długo jak program i sam przebieg proces przekazu kontrolowany jest przez wysyłającego zakwalifikować można tego rodzaju przekazywanie, nawet jeśli następuje z niewielkim czasowym opóźnieniem, do kategorii nadania<sup>242</sup>.

Uwagi na temat eksploatacji w sieci i poprzez sieć utworów wskazują na obszerność i znaczenie tego zagadnienia. Samo udostępnienie dzieła w Internecie stanowi czyn wkraczający w przyznane autorowi prawa majątkowe. Określenie jednak skutków owego działania jest bardzo trudne. Osobną kwestią jest ustalenie skutków prawnych związanych z utrwalonymi na przejściowy okres czasu czy też wręcz efemerycznymi zapisami elektronicznymi. Czy powinny być one zakwalifikowane do objętej treścią prawa autorskiego kategorii zwielokrotnienia? Czy udostępnienie utworu w sieci komputerowej zaliczyć do całkiem nowego pola eksploatacji?

Konieczne staje się ponowne zdefiniowanie takich pojęć jak egzemplarz, zwielokrotnienie, wprowadzenie do obrotu, rozpowszechnianie. Należy także położyć nacisk na zaakceptowanie niematerialności tak samego utworu jak i jego egzemplarza.

## Dozwolony użytek

Wszystkie ustawy o prawie autorskim zawierają przepisy regulujące zakres dozwolonego korzystania z chronionych utworów. Nie inaczej jest w polskiej ustawie o prawie autorskim i prawach pokrewnych. Powołując się na owe przepisy można (odpłatnie lub nie) posługiwać się rozpowszechnionym utworem lub jego częścią bez zgody uprawnionego. Ograniczenia w prawach autorskich mają swe uzasadnienie tak w osobistych interesach użytkowników (dozwolony użytek prywatny) jak i interesach społecznych (dozwolony użytek publiczny) – rozwój edukacji, nauki, dostępu do kultury czy informacji. Czy ograniczenia te znajdują jednak zastosowanie do utworów rozpowszechnianych w sieciach komputerowych?<sup>243</sup>

---

<sup>241</sup> Coraz bardziej popularne są usługi telewizyjne w systemie *pay-per-view*, *pay-per-channel*, *video-on demand*, *near-video-on-demand*, czy też oglądanie wielu kanałów jednocześnie).

<sup>242</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.151, zob. także V. Makarenko *TV Internet- oferta polskich stacji telewizyjnych*, „Gazeta Wyborcza” z 27.12.2000 r.

<sup>243</sup> W Polsce, gdzie dozwolony użytek uregulowano poprzez kazuistyczne licencje ustawowe trudno jest nadać za wszelkimi nowymi formami korzystania z utworów. Lepszym rozwiązaniem wydaje się być instytucja *fair*

Nie można nie zauważyć korzyści, które społeczeństwo może uzyskać dzięki instytucji dozwolonego użytku. Pojawiają się one, przede wszystkim, w trzech dziedzinach:

- a) dostępu do informacji,
- b) prywatności,
- c) swobody wypowiedzi.

### Dozwolony użytek publiczny

Rozróżnić możemy w tej materii dwa zasadnicze przeciwstawne punkty widzenia. Pierwszy z ich dotyczy ograniczenia swobody korzystania z chronionych utworów. Porusza się tu problem łatwości i szybkości dostępu do ogromnych zasobów materiałów- co wiąże się niebezpieczeństwem łamania prawa autorskich na wielką skalę.

Drugi natomiast to podejście liberalne. Aspekty społeczne, kulturowe, dostępu informacji powodują rozszerzającą interpretację dozwolonego użytku publicznego to drugie podejście korygują postanowienia generalne stanowiące regułę (art.35 pr. autorskiego), iż „dozwolony użytek nie może naruszać normalnego korzystania z utworu lub godzić w słuszne interesy twórcy”<sup>244</sup>.

Wydaje się, iż cztery podstawowe zagadnienia mogą dotyczyć swobodnego użytku publicznego w sieciach komputerowych. Są to mianowicie:

- prawo rozpowszechniania w Internecie – art. 25 pr. aut.,
- sprawozdania o aktualnych wydarzeniach – art. 26,
- cytaty i antologie – art. 29,
- publikowanie utworów plastycznych w encyklopediach użytkowanych w sieciach – art. 33 ust. 3.

Kwestia licencji ustawowych dla instytucji naukowych, bibliotek, archiwów i szkół czy ośrodków informacji i dokumentacji naukowo- technicznej stwarza wątpliwości przy ocenie różnych form działalności realizowanych w oparciu o te licencje w środowisku komputerowym<sup>245</sup>.

Kontrowersyjne jest natomiast czy uprawnienie do korzystania (art. 27) , udostępniania (art. 28) i rozpowszechniania (art. 30) obejmuje także wprowadzenie tych utworów do „powszechnych” sieci komputerowych. Analiza art.35 stwarza duże wątpliwości w przypadku dopuszczalności powoływania się na omawiane licencje w sieciach komputerowych<sup>246</sup>.

---

*use* , która jest bardziej elastyczna, wyraża bowiem sferę dozwolonego korzystania z utworów, patrz też J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.153.

<sup>244</sup> Przytoczona regulacja stwarza 3 zasadnicze problemy co do stosowania tak ujętego znaczenia:

1.Niektóre postacie dozwolonego użytku niejako z założenia godzą w normalne korzystanie z utworu i słuszne interesy twórcy.

2.Czy art. 35 pr. autorskiego może być stosowany generalnie czy też jednostkowo?

3 Jak art. 35 będzie się miał w stosunku do pól eksploatacji nie znanych lub dostatecznie nie rozpowszechnionych w momencie uchwalenia ustawy?

<sup>245</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.158.

<sup>246</sup> Por. J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.158-160.

## Użytek osobisty

Podstawą prawną dozwolonego użytku prywatnego jest art. 23 prawa autorskiego. Nie można ograniczać tej instytucji w dotychczasowym ujęciu co do eksploatacji prowadzonej w sieciach komputerowych. Z omawianą licencją ustawową na rzecz użytku prywatnego pozostają w swoistym związku regulacje prawa mające za cel złagodzenie ujemnych skutków ekonomicznego występowania po stronie uprawnionych w rezultacie masowego, nie poddającego się kontroli, kopiowania utworów dla celów użytku osobistego.<sup>247</sup>

Reguluje tą kwestię art. 20 prawa autorskiego. Obciążenia producentów i importerów magnetofonów i magnetowidów oraz innych urządzeń czy też nośników (płyty, kaset, dyskietek) opłatami na rzecz twórców ma zmniejszać owe ujemne skutki działania.

Jednak na tym polu pojawiają się pytania dlaczego producenci komputerów czy programów komputerowych umożliwiających dozwolony użytek z utworów dostępnych w sieciach komputerowych nie są obciążeni owym obowiązkiem? Dlaczego są oni traktowani preferencyjnie? Ciekawą kwestię poruszają autorzy pracy *Internet a prawo* (str. 161-162) – stosowanie instytucji dozwolonego użytku osobistego w sferze zapisu cyfrowego. Zachęcam do przeczytania tych ciekawych rozważań.

Dyskusja o dozwolonym użytku prywatnym będzie toczyć się wokół dwóch poglądów. Pierwszym z nich jest zachowanie status quo i podkreślanie, iż technika zapisu utworu i zapisu kopii, o ile tylko cała eksploatacja mieści się w ramach użytku osobistego, nie powinna mieć tu znaczenia. Drugi natomiast wskazuje na analogię z programem komputerowym. Domaga się on statuowania całkowitego zakazu sporządzania kopii cyfrowych z utworów utrwalanych w taki sposób.<sup>248</sup>

## Umowy, tworzenie i eksploatacja produktów multimedialnych

Podczas eksploatacji i tworzenia utworów w Internecie konieczne są w wielu przypadkach umowy, które mają za przedmiot prawa autorskie i prawa pokrewne<sup>249</sup>. Można je ująć w dwie zasadnicze grupy:

- pierwsza dotyczy utworów tradycyjnych, chronionych przez prawo autorskie, są one rozpowszechniane za pomocą sieci komputerowych przy wykorzystaniu techniki cyfrowej<sup>250</sup>
- druga grupa związana jest z tworzeniem i eksploatacją „nowych kategorii utworów” (przedstawiłem je w części pracy poświęconej przedmiotowi prawa autorskiego).

Wśród tej drugiej grupy największe problemy powstają przy produktach multimedialnych- dobra niematerialne złożone z różnych mediów, z materiałów należących do odmiennych dziedzin sztuki i posługujących się różnymi formami

<sup>247</sup> Ibidem, s.160-161.

<sup>248</sup> Ibidem, s.163.

<sup>249</sup> Z reguły powstaje potrzebna eksploatacji dóbr objętych ochroną prawa pokrewnych. Z uwagi jednak na duże podobieństwo tej ochrony do praw autorskich wszystkie rozważania będą miały zastosowanie także i do prawa pokrewnych.

<sup>250</sup> Problem dotyczący pól eksploatacyjnych poruszałem już wcześniej.

wyrazu (słowa, dźwięk, obraz, film), dla których eksploatacji niezbędny jest komputer.<sup>251</sup> Czy digitalizacja utworu stanowi nowe, całkowicie odrębne, uprawnienie autora, które jest niezależne od ogólnego prawa do reprodukcji?

Przy tworzeniu dzieł multimedialnych wyróżnić możemy trzy grupy umów:

- umowy z twórcą utworu multimedialnego,
- umowy z autorami utworów stworzonych na zamówienie producenta dzieła multimedialnego,
- umowy z autorami utworów służących, wykorzystywanych w utworze multimedialnym <sup>252</sup>.

Producent utworu multimedialnego zawierający umowę z autorem (czy współautorem) utworu powinien uwzględnić interesy nie tylko twórcy lecz również autorów koncepcji, układu, doboru składników produktu multimedialnego. Nie może pominąć także innych współtwórców, których wkłady nie są zdatne do wyodrębnienia. Jak wspomniałem istnieją wątpliwości co do przypisania utworów multimedialnych do znanego prawa autorskiego rodzaju dzieł. Powstaje pytanie czy nabycie praw autorskich przez producenta takiego dzieła ma charakter pochodny czy też pierwotny. Odpowiedź na to pytanie nie jest jedynie teoretyczna. W zależności od odpowiedzi zaistnieją różne skutki prawne związane z kształtowaniem treści umów zawieranych z osobami wnoszącymi twórcze wkłady do utworów multimedialnych.

Włączenie do dzieła multimedialnego materiałów już istniejących czy też dostępnych informacji nie jest zawsze związane ze zgodą czy zapłatą wynagrodzenia. Nie jest potrzebne uzyskanie takiej zgody w przypadkach włączenia do dzieła wytworów nie stanowiących utworów w rozumieniu prawa autorskiego. Dopuszczalne jest także wykorzystywanie utworów co do których wygasły już prawa autorskie.<sup>253</sup>

Konieczne staje się również uwzględnianie dozwolonego użytku publicznego (art. 29 ust. 1 i 2 oraz art. 33 pkt. 3 prawa autorskiego). W przypadku inkorporowania utworów do dzieła multimedialnego w oparciu o umowy możemy wyróżnić dwa zasadnicze zagadnienia:

1. Utwory specjalnie stworzone.

Nabycie praw przez producenta następuje w sposób pochodny. Umowy zawierane przez producenta z autorami takich utworów będą decydować o zakresie dopuszczalnej eksploatacji

2. Utwory, które już istniały.

Największe problemy wiążą się właśnie z tą grupą utworów. Trudności z ustaleniem podmiotu uprawnionego do udzielenia licencji, uzyskanie od niego zgody oraz nadania umowie określonej treści<sup>254</sup> stanowią, że często producenci utworów multimedialnych rezygnują z włączenia takich dzieł na korzyść zamawianych utworów, które często są gorszej jakości.<sup>255</sup>

---

<sup>251</sup> Definicja przytoczona została za: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.165.

<sup>252</sup> Podział za J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.165.

<sup>253</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.168.

<sup>254</sup> Na temat treści umowy z twórcą dzieła zob. J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.174-177.

<sup>255</sup> Ibidem, s.170-173.

Licencja autorska na korzystanie z utworów w sieci komputerowej to zagadnienie, które budzi szczególne zainteresowanie. Umowy zawierane przez uprawnionych z tytułu praw autorskich z bezpośrednim dostawcą utworu do sieci komputerowej mają za zadanie udzielenie zezwolenia na eksploatację przez licencjobiorcę utworu w systemie *on line*, a także na korzystanie z nich przez końcowych użytkowników.<sup>256</sup> Natomiast do problematyki programu komputerowego w utworze multimedialnym (który steruje tego typu dziełem) znajdują zastosowanie ogólne zasady redakcji odpowiednich umów komputerowych. Posiadają one odrębną specyfikę z uwagi na przyjętą w polskim prawie autorskim ochronę programów komputerowych.

Trudności w tworzeniu produktów multimedialnych są znaczące. Powodują one niekiedy iż wydawcy takich produktów nie decydują się na korzystanie z już istniejących utworów. Niejasności na rynku praw autorskich, zawile przepisy i ogólnie „zły klimat” przy tworzeniu podobnych dzieł (związane z tym polem eksploatacji obawy twórców) nie sprzyjają szybkiemu rozwojowi dzieł multimedialnych<sup>257</sup>.

Wiele zagadnień związanych z Internetem i prawem autorskim wymaga szerszego omówienia. Rozwiązania międzynarodowe (w tym UE) dotyczące sieci przedstawiłem w rozdziale II, natomiast problemy baz danych oraz adresów internetowych staną się przedmiotem rozdziału V.

Prawo autorskie jest bodajże najbardziej w cyberprzestrzeni widziane. Z uwagi na posługiwanie się tekstem, obrazem i dźwiękiem Internet stwarza wiele wątpliwości na gruncie tej gałęzi prawa. Skromne ramy mej pracy niestety nie pozwalają skupić się uważniej na skutkach wpływu Internetu na prawo autorskie. Daje się jednak zauważyć, iż samo prawo autorskie będzie odgrywać w stosunku do sieci coraz bardziej znaczącą rolę. Wynika to z jednej strony z samego przedmiotu, którym się ono zajmuje, a z drugiej z cechy ustawodawstwa autorskiego, wychodzącego naprzeciw nowym aspektom.

---

<sup>256</sup> Ibidem, s.178.

<sup>257</sup> Ibidem, s. 179-182.

# Rozdział V.

## Adresy internetowe, bazy danych i ich ochrona

### 1. Domeny internetowe

#### Uwagi wstępne oraz znaki towarowe

Bezpośrednio z funkcjonowaniem Internetu wiąże się zagadnienie domen internetowych (*Internet Domain Names*) oraz ich ochrony. Internet jest ogólnosiątkowym zbiorem połączonych między sobą sieci komputerowych w oparciu o protokół TCP/IP (*Transmission Control Protocol/Internet Protocol*) używany do powiązania różnych sieci fizycznych w jedną sieć logiczną<sup>258</sup>. Jednak dla ułatwienia ludziom posługiwania się stronami WWW powstał system domen<sup>259</sup>. Powstał, podkreślić należy nie w celu identyfikacji znaków towarowych lecz w celu uczynienia surfowania w sieci łatwiejszym.

Sam adres-domena służy także niejednokrotnie identyfikacji samego użytkownika poprzez odwołanie się do jego nazwy handlowej czy znaku towarowego. Adresy internetowe zazwyczaj dzieli się na adresy poczty elektronicznej i adresy stron WWW.

1. Adres poczty elektronicznej (*e-mail*) posiada następujące elementy: przedzielonego znakiem „@” identyfikatora użytkownika (*ID, username, login name*) i adresu domenowego<sup>260</sup>.

2. Adres strony WWW zapisuje się przy wykorzystaniu URL-u (Uniform Resource Locator)- częścią URL-u jest adres domenowy. Klasyczna domena składa się z następujących elementów<sup>261</sup>: oznaczenia protokołu transmisji (1), ogranicznika (2), loginowego oznaczenia serwera WWW zastępującego nazwę hosta (3), domeny III poziomu (4), domeny II poziomu (5), Toplevel domeny (6), oraz nazwy katalogu na serwerze (7) i strony html (8) np.:

`http1://2www3.znak@4.com.5pl6/SITE/7info.html8`

<sup>258</sup>R. Chmura, W. Włodarczyk, *Bezprawne używanie zarejestrowanych znaków towarowych w adresach domenowych w świetle ustawy o znakach towarowych*, [w:] R. Skubisz (red): *Internet- problemy prawne*, op. cit., s.85.

<sup>259</sup> D.J. Loundy, *A Primer on Trademarks Law and Internet Addresses*, 15 John Marshal J. Of Computer and Info Law 465(1997).

<sup>260</sup> Całkowicie odmienne są zasady przyznawania adresów poczty elektronicznej od zasad przyznawania domen internetowych.

<sup>261</sup> Patrz szerzej na ten temat: R. Chmura, W. Włodarczyk, *Bezprawne używanie zarejestrowanych znaków towarowych w adresach domenowych w świetle ustawy o znakach towarowych*, [w:] R. Skubisz (red): *Internet- problemy prawne*, op. cit., s.88-94. Istnieje 244 domen krajowych np. dla Polski „.pl”, pro – wejdą one do użytku prawdopodobnie w selectoins for law TOP- Level Domains [www.icann.org/announcements/icann/pr16nor00.htm](http://www.icann.org/announcements/icann/pr16nor00.htm). oraz G.Sowela, *Zmi.ana adre.su*, „Rzeczpospolita” z dnia 23.11.2000 r. oraz R. Chmura, W. Włodarczyk, *Bezprawne używanie zarejestrowanych znaków towarowych*

*w adresach domenowych w świetle ustawy o znakach towarowych*, [w:] R. Skubisz (red): *Internet- problemy prawne*, op. cit., s. 92-93.

Komercjalizacja Internetu, szerokie zastosowanie do transakcji handlowych, marketingowych i reklamowych stwarza warunki do szybkiego rozwoju rynku domen.

Tak kształtuje się ilość przyznawanych i funkcjonujących w Internecie „polskich” domen:

Tabela 2. Statystyka domen w ostatnich 4 tygodniach z rozbiem na główne domeny funkcyjne:

Data	pl	com.pl	net.pl	org.pl	edu.pl	gov.pl	mil.pl	razem
2001-04-15	45427	48920	2058	1207	687	192	25	98516
2001-04-08	45271	48692	2016	1190	683	191	25	98068
2001-04-01	44716	48325	1984	1172	673	191	25	97086
2001-03-25	43909	48006	1960	1162	665	190	25	95917

Copyright © 1999-2000 WEB Corporation Polska Sp. z o.o.  
 Źródło: NetNames Polska - <http://www.netnames.pl>

Jeżeli do tego uwzględnimy ponadkrajowy charakter sieci komputerowych, to łatwo przewidzieć, iż posługiwanie się adresami internetowymi znajduje się w obszarze działania tych dziedzin prawa, które zajmują się ochroną znaków towarowych, oznaczaniem miejsca pochodzenia towaru, ochroną znaków towarowych, a także dóbr osobistych. Kto jednak rozdziela (przydziela) i rozpowszechnia adresy internetowe? Czy z uwagi na globalny charakter sieci jest to jedna instytucja?<sup>268</sup> Niestety takiej jednej instytucji nie ma. W Niemczech domeny bada czy nie są już używane centrum Informatyczne w Karlsruhe (DENIC) w Stanach Zjednoczonych jest to InterNIC (Internet Network Information Center's Registration Services) a w Polsce NASK – Naukowa i Akademicka Sieć Komputerowa. NASK odmawia rejestracji domeny w trzech wypadkach:

1. gdy jest już zarejestrowana w NASK,
2. gdy został złożony wniosek o zarejestrowanie identycznej domeny a postępowanie rejestracyjne jest w toku,
3. jest nazwą podmiotu prawnego nie związaną z wnioskodawcą.<sup>269</sup>

<sup>268</sup> Politykę nazewnictwa w Internecie kontroluje organizacja ICANN – Internet Corporation for Assigned Names and Numbers – stworzona w październiku 1998 r. przez koalicję biznesu internetowego, informatyków, naukowców i użytkowników. Jest ona niezależną korporacją ds. nazewnictwa.

<sup>269</sup>Za: R. Chmura, W. Włodarczyk, *Bezprawne używanie zarejestrowanych znaków towarowych w adresach domenowych w świetle ustawy o znakach towarowych*, [w:] R. Skubisz (red): *Internet- problemy prawne*, op. cit., s.96.

Rejestracja następuje, co szczególnie ważne, według kolejności zgłoszeń. NASK zastrzega sobie jedynie prawo do usunięcia delegacji domeny, gdy zostanie mu doręczona decyzja sądu patentowego lub wyrok sądu potwierdzający prawa trzeciego podmiotu do nazwy.

Domeny służą oznaczaniu urządzenia nie osoby i użytkownika. Niektórzy uważają, że można je nawet porównać do numeru telefonicznego, w tym jednak przypadku domena jest swobodnie wybierana, kształtowana. Jest łatwiejsza do zapamiętania (oczywiście nie zawsze) oraz nie jest zestawem przypadkowych liczb. Dobrze wybrany adres internetowy może także - z oznaczeniem przedsiębiorstwa lub samodzielnie obok niego - pełnić w praktyce funkcję handlowej identyfikacji przedsiębiorstwa gospodarczego. Posługiwanie się adresami internetowymi stwarza problemy zasadniczo z dwóch powodów:

- istnieją ogromne wątpliwości co do relacji adresów do znanych sposobów oznaczania pochodzenia towarów czy usług, zwłaszcza znaków towarowych,
- społeczność internetowa stale preferuje metodę samoregulacji problemu<sup>270</sup>.

Relacje między znakami towarowymi a domenami internetowymi są bardzo skomplikowane. Autorzy pracy *Internet a prawo* wyróżniają trzy zasadnicze problemy:

1. Międzynarodowy charakter sieci komputerowych. Przesądza to o międzynarodowym wykorzystaniu adresów. Znaki towarowe mogą być także eksploatowane lokalnie wynikiem czego jest zawłaszczanie domen internetowych.
2. Istnienie tylko 14 generycznych Top Level Domain wobec 42 klas znaków towarowych odnoszących się do określonych grup towarów i usług.
3. Zakazu rejestrowania nie tylko takich samych adresów, które są identyczne z już zarejestrowanymi lecz również podobnych do nich, które już zostały objęte domeną<sup>271</sup>.

Spójrzmy dokładniej na zachodzące relacje między znakiem towarowym a domenami internetowymi. Wyróżnić możemy co najmniej pięć podstawowych zagadnień:

1. Czy za naruszenie prawa do zarejestrowanego znaku towarowego można uznać wykorzystanie go przez osobę trzecią (konkurenta) jako składnika jego własnego adresu internetowego?<sup>272</sup> Przepis art. 13 ust.1 ustawy o znakach towarowych<sup>273</sup> określa pozytywnie uprawnienie używania, które nabywa podmiot prawa z chwilą rejestracji znaku towarowego. Uprawniony posiada wyłączność na posługiwanie się danym znakiem towarowym w obrocie gospodarczym na terytorium Rzeczypospolitej Polskiej dla towarów objętych rejestracją<sup>274</sup>.

<sup>270</sup> Ibidem, s. 263.

<sup>271</sup> Ibidem.

<sup>272</sup> Zob. też J. Ożogalska, *Prawne problemy posługiwania się adresami (domenami) internetowymi w obrocie gospodarczym*, „Radca Prawny” 01/2001. oraz R. Chmura, W. Włodarczyk, *Bezprawne używanie zarejestrowanych znaków towarowych w adresach domenowych w świetle ustawy o znakach towarowych*, [w:] R. Skubisz (red): *Internet- problemy prawne*, op. cit., s.98.

<sup>273</sup> Dalej w tekście „u.z.t.”. Ustawa z 31.01.1985 r. o znakach towarowych (Dz. U. 85.5.17.).

<sup>274</sup> Podkreślić należy, iż prawo z rejestracji udziela wyłączności na komercyjne (w obrocie gospodarczym) używanie takiego oznaczenia, dotyczy ona tylko towarów objętych rejestracją, oraz ograniczona jest do

Naruszeniem prawa będzie więc posługiwanie się czyjś znakiem towarowym, jeśli stanowi on element charakterystyczny danej strony WWW. Możliwe są bardziej ostrożne oceny w tej kwestii. Według nich o naruszeniu praw do znaku towarowego będzie można mówić w momencie, gdy adres internetowy jest eksponowany na stronie WWW w ten sposób, aby przykuć uwagę na przyjęty do niego cudzy znak towarowy<sup>275</sup> - art. 24 ust. 1 pkt 2 u.z.t.

2. Drugą kwestią jest posługiwanie się zarejestrowanymi znakami towarowymi jako składnikami własnych adresów internetowych w relacjach międzynarodowych. Należy rozpatrzyć tu sytuację, gdy wspomniany adres jest wprowadzony do państwa, w którym nie ma ochrony danego znaku towarowego. Globalny charakter Internetu podważa jednak zasadę terytorialności ochrony wynikającej z rejestracji znaku towarowego. Jest on przecież eksploatowany „równocześnie” na całym świecie. Nie ma podstaw do uznania takiego zachowania za naruszenie praw wynikających z rejestracji znaku towarowego, gdy dany podmiot nie prowadzi działalności gospodarczej na rynku określonego kraju, w którym nastąpiła rejestracja trudno jednak znaleźć jedno rozwiązanie dotyczące tej problematyki.

3. Trzecim zagadnieniem jest używanie znaku towarowego przez inny podmiot, gdy prowadzi on działalność gospodarczą w innej dziedzinie niż podmiot uprawniony z zarejestrowanego znaku towarowego. Powszechnie uznaje się takie działanie za dopuszczalne<sup>276</sup>.

4. Czy adres internetowy może zostać zarejestrowany jako znak towarowy? O ile spełnione są wszystkie przesłanki ustawowe należy przychylić się do pozytywnej odpowiedzi na tak zadane pytanie. Wiązać się to będzie z wykorzystaniem takiego znaku towarowego przy oferowaniu odpowiednich usług i towarów<sup>277</sup>.

5. Ostatnim zagadnieniem są tzw. *meta-tags* czyli opisy stron WWW w języku HTML, które ułatwiają znalezienie danej strony przez posłużenie się wyszukiwarką internetową. Często zarejestrowanymi znakami towarowymi posługują się inne firmy, które właśnie poprzez *meta-tags* próbują dotrzeć do użytkowników Internetu. Czy w takiej sytuacji dochodzi do naruszenia ochrony znaku towarowego? - pytają autorzy pracy *Internet a prawo*. Będziemy mieli tu raczej do czynienia z reklamą towarów czy usług objętych zakazem prawa z rejestrowanego danego znaku. Traktować to należy jako naruszenie prawa wyłącznego<sup>278</sup>.

---

terytorium RP. Ponadto art. 13 u.z.t. przewiduje, iż nazwa znaku towarowego może polegać na m.in. : „umieszczeniu go na dokumentach związanych z wprowadzeniem oznaczonego towaru do obrotu” – chodzi tu o listy handlowe, zamówienia, katalogi, informatory oraz o posługiwanie się nim w środkach masowego przekazu w celu reklamy – R. Skubisz, *Prawo znaków towarowych- komentarz*, Warszawa 1997 r., s. 128.

<sup>275</sup> Por. J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 265.

<sup>276</sup> Ibidem, s. 266-267. Przytoczona tam sprawa *Avent Inc vs. Isoart Ltd* z Wielkiej Brytanii potwierdza takie właśnie rozwiązanie tej kwestii.

<sup>277</sup> R. Chmura, W. Włodarczyk, *Bezprawne używanie zarejestrowanych znaków towarowych w adresach domenowych w świetle ustawy o znakach towarowych*, [w:] R. Skubisz (red): *Internet- problemy prawne*, op. cit., s.104.

<sup>278</sup> Zob. J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 268.

## Nieuczciwa konkurencja

Polska ustawa o nieuczciwej konkurencji z 16.04.1993 r. posiada duże znaczenie jeśli chodzi o posługiwanie się „cudzymi” adresami internetowymi (domenami). Wzrost wartości takich adresów powoduje, iż problem ten nabiera coraz wyraźniejszego kształtu. Zasadniczą kwestią jest odróżnienie oparcia swego roszczenia na przepisach ustawy o nieuczciwej konkurencji od roszczeń opartych na ustawie o znakach towarowych. Ważnym jest ustalenie wykorzystywania cudzego znaku towarowego jako elementu adresu internetowego w taki sposób, który nie stanowi naruszenia przepisów owej drugiej ustawy lecz skutkuje:

- a) wprowadzeniem użytkownika Internetu w błąd co do pochodzenia oferty,
- b) osłabia wyraźnie wartość wykorzystywanego w adresie znaku,
- c) wyłącza możliwość wprowadzenia własnego znaku towarowego do domeny internetowej.

Powszechnie znanym i budzącym wiele kontrowersji jest tzw. *cybersquatting* nazywany czasami „dzikim osadnictwem w sieci”<sup>279</sup>. Działanie takie polega na rejestrowaniu wybranej nazwy jako adresu internetowego, który zawiera element cudzego znaku towarowego. Ma to na celu zmuszenie danego podmiotu do zapłaty określonej kwoty za wykupienie praw do takiej domeny.<sup>280</sup> W Stanach Zjednoczonych praktyka ta stała się przedmiotem wielu spraw sądowych. Kwestia wykorzystywania cudzego znaku towarowego jako własnego adresu internetowego została uregulowana m.in. w Federal Dillution Act z 1995 r. (15 U.S.C. 1125 (c))<sup>281</sup>. Ustawa ta chroni uznane znaki towarowe przed ich wykorzystaniem przez osoby trzecie w celach handlowych, które powodują osłabienie – *dillution*<sup>282 283</sup>(czasami tłumaczone jako rozwodnienie) – wartości wyróżniającej znak. Chodzi zatem nie o wyłączenie możliwości wprowadzania klientów w błąd lecz o osłabienie wartości rynkowej, wartości marketingowej sławnego znaku<sup>284</sup>. Na gruncie *cybersquattings* szczególne znane stały się dwie sprawy sądowe.

---

<sup>279</sup> K.Kort, *Dziki osadnictwo w sieci*, „Gazeta Wyborcza” z 06.03.2000 r., przedruk z „Wall Street Journal Europe”.

<sup>280</sup> W grę wchodzi czasami bardzo duże pieniądze np. firma eCompanies zapłaciła 7,5 mln USD za prawa do domeny business.com. Patrz: D. Gajos, *Niech rozsądzi nas arbiter*, „Rzeczpospolita” z dnia 30.11.2000 r.

<sup>281</sup> Zob. J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 269 oraz D.J. Loundy, *A Primer on Trademarks Law and Internet Addresses*, 15 John Marshal J. Of Computer and Info Law 465(1997), s. 474.

<sup>282</sup> J.L. Loundy wyróżnia kilka rodzajów *dillution*: miejsc, w których owo „rozwodnienie” może nastąpić i spowodować chaos w przypadku domen. Jednym z takich budzących kontrowersje spraw jest umieszczenie zera „0” w nazwach domen, np. micros0ft.com. użycie zera wskazuje za sposoby omijania przepisów. Takich rozwiązań jest oczywiście więcej. J.L. Loundy podaje jeszcze dwa przykłady: honda.purdue.edu oraz nexchi.com/~sony . Te sprawy pokazują jak trudno jest czasami oprzeć się na sztywnych przepisach ustawy w przypadku Internetu. W pozostałych przykładach można bowiem powoływać się na (sprawy miały miejsce w USA) pierwszą poprawkę do konstytucji Stanów Zjednoczonych. Prowadzi to do parodii ochrony znaków towarowych. Taka ochrona nie jest więc absolutna. Na przykład niektóre sądy twierdzą, że I poprawka niekoniecznie wyprowadza prawo do naruszenia praw posiadaczy znaków towarowych tak długo jak są to odpowiednio alternatywne wyrazy myśli dotyczące wymiany poglądów danych osób. D.J. Loundy, *A Primer on Trademarks Law and Internet Addresses*, 15 John Marshal J. Of Computer and Info Law 465(1997), s. 484.

<sup>284</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 269-270.

## 1. **Intermatic Inc vs. Toeppen**<sup>285</sup>.

Toeppen zarejestrował domenę (Intermatic.com) za znakiem towarowym Intermatic i jednocześnie wykorzystywał ją do prowadzenia działalności handlowej (sprzedaży oprogramowania). Sąd przychylił się do zdania powoda, iż osłabiło takie działanie zdolność znaku towarowego do identyfikacji i rozróżniania towarów i usług. Spowodowane to zostało dwoma okolicznościami:

a) faktycznym odebraniem możliwości rejestracji i używania znaku jako elementu adresu internetowego przez Intermatic

b) stałym stosowaniem oznaczenia podobnego do innej klasy towarów<sup>286</sup>.

Sąd zakwalifikował działanie Toeppena jako „*commercial use*” oraz nakazał mu przeniesienie adresu na rzecz powoda.

## 2. Drugą sprawą jest: **Panavision vs. Toeppen** <sup>287</sup>.

Toeppen zarejestrował domenę panavision.com. zamieścił na tej stronie widok miasta Pana w Illinois. Nie prowadził tam (na stronie WWW) żadnej działalności handlowej. Gdy jednak Panavision zasugerowało odstąpienie nazwy Toeppen zażądał 13 tys. USD. Później natomiast zarejestrował jeszcze domenę panaflex.com. na stronie tej umieścił tylko jedno słowo: „Hello”. Sąd uznał, iż działanie Toeppena narusza interes konsumentów przez to, iż utrudnia im znalezienie WWW firmy Panavision. <sup>288 289</sup>.

Polska ustawa o nieuczciwej konkurencji jasno określa takie postępowanie jako bezprawne. Mamy tu do czynienia z działaniem sprzecznym z dobrymi obyczajami z perspektywy podmiotów używających znaki towarowe, z postępowaniem, które ewidentnie narusza lub zagraża ich interesom (art. 3 u.z.n.k.) <sup>290</sup>

Jednak należy wtedy wykazać, iż takie działanie było zamierzone. Można także powołać się na art. 5 u.z.n.k., gdy podmiot używa w domenie oznaczenia identycznego lub podobnego, które stanowi znak towarowy innej firmy, bez porozumienia z nią. W przypadku zastosowania w domenie nazwy geograficznej, gdy fałszywie sugeruje ona związek posiadacza adresu z danym rejonem można powołać się na art. 8 ustawy. Z kolei zamieszczenie w adresach internetowych elementów myląco oznaczających pochodzenie towarów można zakwalifikować jako reklamę wprowadzającą w błąd. Będzie miał tu zastosowanie art. 16 ust. 2 u.z.n.k.

Wydaje się więc, że kwestia ta dostatecznie została w polskim prawie uregulowana (można przy tym powoływać się na postanowienia kodeksu handlowego w sprawie firmy oraz na art. 23 i 24 k.c. czy na omówioną przeze mnie ustawę o znakach towarowych). Jak to jednak jest, iż polskie sądy jeszcze nie

<sup>285</sup> Intermatic Inc vs. Toeppen 96 C 1982, 1996 U.S. Dist. Lexis 14878 (ND III Oct. 3. 1996)..

<sup>286</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.270.

<sup>287</sup> Panavision Int'l L.p. vs. Toeppen 1996 WL 653736 (C.D. Calif. Nov. 05, 1996.

<sup>288</sup> Podobnych spraw jest z roku na rok więcej. Zauważyć można, iż linia orzecznictwa wcale nie jest jeszcze ustalona. Sprawy takie pojawiają się tak na gruncie systemu prawa stanowionego jak i *common law*. Nawet na obszarze jednego państwa zdarzają się całkowicie odmienne orzeczenia, np. sprawa Harrods Ltd v. UK Network Services Ltd. oraz Avnet Inc. V. Isoart Ltd.

<sup>289</sup> Na temat spraw przeciwko Toeppenowi zobacz: D.J. Loundy, *A Primer on Trademarks Law and Internet Addresses*, 15 John Marshal J. Of Computer and Info Law 465(1997), s. 447-483.

<sup>290</sup> Zob. J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.271.

orzekały w podobnych tego typu sprawach? Odgrywa tu znaczącą rolę brak odpowiedniego orzecznictwa, wysokie koszty i przede wszystkim niepewny rezultat danej sprawy.<sup>291</sup>

Innym ciekawym problemem na gruncie ustawy o zwalczaniu nieuczciwej konkurencji jest ocena dopuszczalnego tworzenie tzw. linków zawierających cudze znaki towarowe.<sup>292</sup> Trudno na gruncie prawa polskiego zakazać stosowania takich odnośników.

Wykorzystywanie w adresach internetowych nazwisk, firm czy innych nazw może prowadzić do naruszenia dóbr osobistych osób fizycznych czy prawnych. Takie działanie jednak musi spełniać określone przesłanki:

- dany adres powinien zawierać cudze nazwisko, firmę, nazwę przedsiębiorstwa, pod którą ktoś prowadzi działalność gospodarczą,
- będzie przez to narażał te podmioty na utratę dobrego imienia lub renomy (pogląd ów został ustalony na gruncie orzecznictwa niemieckiego).

Do naruszenia może dojść tylko wówczas, gdy sposób korzystania z cudzego dobra we własnym adresie internetowym może grozić ujemnymi skutkami dysponentowi tych dóbr<sup>293</sup>. Przykładowe ujemne skutki to: utrata dobrego imienia, wiarygodności tak handlowej, jak i prywatnej, utrata renomy.

Postępowaniem, które prowadzi do takich właśnie celów może być umieszczenie pod danym adresem informacji o treściach kompromitujących dany podmiot, ośmieszających czy też prowadzenie działalności gospodarczej innej – gorszej – jakości. Kwestę dóbr osobistych w Internecie porusza orzeczenie sądu niemieckiego w sprawie heidelberg.de. dokładnie omówione zostało ono w pracy J. Barty i R. Markiewicza *Internet a prawo*<sup>294</sup>.

Na gruncie prawa polskiego w podobnych sytuacjach będą miały zastosowanie art. 23 i 24 k.c. (w związku z art. 43 k.c.). odpowiedzialność uzależniona została od wykazania, iż posługiwanie się przez pozwanego w domenie internetowej cudzą nazwą (nazwą powoda) spowodowało utratę przez niego renomy przedsiębiorstwa rozumianej jako „ogół pozytywnych wyobrażeń lub ocen konsumentów o wyrobach tego przedsiębiorstwa”<sup>295</sup>.

Kontrowersje powstają nie tylko przy domenach internetowych. Również adresy poczty elektronicznej mogą powodować duże problemy na podstawie przepisów o ochronie dóbr osobistych czy ochrony danych osobowych.<sup>296</sup> Prawny status i podstawa ochrony adresów internetowych nie są jeszcze do końca sprecyzowane. Co prawda ochrona ta następuje na mocy przepisów ustawy o z.n.k. oraz ustawy o znakach towarowych lecz nie jest to zadowalający stan rzeczy. Wskazuje się na potrzebę międzynarodowego uregulowania tego problemu, które

---

<sup>291</sup> Zob. H. Fedorowicz, *Niech rozsądzi nas arbiter, adresy z cudzą firmą*, „Rzeczpospolita” z 02.01.2001 r. oraz J. Ożogalska, *Prawne problemy posługiwania się adresami (domenami) internetowymi w obrocie gospodarczym*, „Radca Prawny” 01/2001, s.26-27.

<sup>292</sup> Na ów temat zobacz więcej: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.272.

<sup>293</sup> J. Ożogalska, *Prawne problemy posługiwania się adresami (domenami) internetowymi w obrocie gospodarczym*, op. cit., s.27.

<sup>294</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.273-274.

<sup>295</sup> Por. wyrok Sądu Apelacyjnego w Warszawie z dn. 19.12.1995 r. sygn. I Acr 1013/95 OSA 1997/4 podają za: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.69-70.

<sup>296</sup> Zob. Ustawa o ochronie danych osobowych Dz.U. z 1997 r. nr 133 poz. 883, zob. też M. Ziętkiewicz, *Chroń go sam*, „Rzeczpospolita” z dn. 20.02.2001 r.

„już w ramach szczególnych postanowień o udzieleniu- przyznaniu domeny eliminowałoby powstawanie takich konfliktów.<sup>297</sup> Sam adres internetowy nie stanowi przedmiotu wyłącznych praw. Wykorzystywanie go jako elementu przez osobę trzecią nie będzie w zasadzie miało charakteru bezprawnego. Jeżeli przesłanki takiego działania zaistnieją wtedy będą miały zastosowanie przepisy o zwalczaniu nieuczciwej konkurencji, najczęściej będzie można powoływać się na art. 3 i 5 ustawy. Z tzw. *secondary meaning* będziemy mieli do czynienia, gdy adres internetowy lub jego charakterystyczny element kojarzony będzie przez potencjalnych klientów z danym produktem lub konkretnym towarem czy usługą. Analogicznie oceny odnoszą się do działań sprzecznych z ustawą o znakach towarowych lub naruszających omówione już przepisy kodeksu cywilnego o dobrach osobistych<sup>298</sup>.

Innym zagadnieniem jest przenoszenie praw do adresów internetowych. Jaka umowa cywilno-prawna znajdzie tu zastosowanie? Treścią takiej umowy nie jest przeniesienie prawa jako takiego. Możemy tu mówić raczej o wycofaniu się, zwolnieniu z dotychczasowej domeny internetowej przez jej dysponenta na rzecz innego podmiotu, który „nabywa” adres. Doktryna dopuszcza takie postępowanie skoro sam adres jest nabywany na zasadzie pierwszeństwa. Podkreśla się, iż nie jest wykluczone, iż sąd jest tu władny do wydania nakazu „przeniesienia” adresu internetowego, a co najmniej nakazu wycofania się z domeny przez używającego ją bezprawnie<sup>299</sup>

## 2. Ochrona baz danych

### Bazy danych i ich ochrona w różnych uregulowaniach

Bazy danych są jednym z najważniejszych produktów dostępnych w Internecie. Autorzy pracy *Internet a prawo* wskazują wręcz na to, iż stanowiły one jedną z głównych przyczyn rozwoju sieci<sup>300</sup>. Łatwość i efektywność korzystania z baz danych za pośrednictwem Internetu to niewątpliwie przyczyny dużej popularności tego typu usług. Jeśli natomiast dodamy to, iż elektroniczne banki danych są tańsze, lepszej jakości oraz wygodniejsze w użyciu odpowiedź na pytanie o zalety takiego przechowywania danych nasuwa się sama. Bazy danych mają duże znaczenie komercyjne dlatego też niezbędne jest zapewnienie im dostatecznej ochrony na polu sieci komputerowych. Przed przystąpieniem do opisanie ochrony baz danych na gruncie prawa autorskiego oraz uregulowań w innych krajach (także organizacji międzynarodowych) spójrzmy na chwilę jak owa ochrona może być zagwarantowana przez inne przepisy. Możemy wyróżnić trzy zasadnicze grupy przepisów:

- dotyczące czynów niedozwolonych według k.c.,
- odpowiedzialność kontraktowa – art.471 k.c.,
- oraz przede wszystkim ustawy o zwalczaniu nieuczciwej konkurencji.

<sup>297</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.276.

<sup>298</sup> Ibidem.

<sup>299</sup> Zob. orzeczenie sądu amerykańskiego w sprawie Toeppen vs. Intermetic.

<sup>300</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.282.

Warto przeanalizować unormowanie ustawy o z.n.k. z punktu widzenia ochrony baz danych w Internecie. Wyprodukowanie bazy danych jest przedsięwzięciem czasochłonnym i pracochłonnym oraz kosztownym. Techniczne możliwości sieci (czy generalnie informatyki) stwarzają niebezpieczeństwo łatwego i szybkiego przejęcia zawartości baz oraz wprowadzenie na rynek konkurencyjnej bazy ze skopiowaną zawartością.<sup>301</sup> Dlatego też to zagadnienie powinno być przedmiotem ochrony ze strony ustawy.

Nie można jednak oprzeć owej ochrony na art. 13 ustawy o z.n.k. Zakazuje on naśladowania gotowego produktu w taki sposób, że kopiowana jest jego zewnętrzna postać za pomocą środków reprodukcji. Hipoteza przepisu wymaga aczkolwiek aby dochodziło do wprowadzenia w błąd odbiorców w materii tożsamości producenta czy produktu.<sup>302</sup>

W takim rozumieniu art. 13 dużą wagę będzie zyskiwała generalna zasada z art. 3 ustawy o z.n.k. Zakazuje ona działania sprzecznego z prawem lub dobrymi obyczajami, jeżeli zagraża to lub narusza interes innego przedsiębiorstwa lub klienta.<sup>303</sup>

Zastanowić się trzeba nad wykładnią dobrych obyczajów oraz nad działaniem pozostającym z nimi w sprzeczności. Same dobre obyczaje nie są normami prawnymi lecz jedynie regułami postępowania. Ich treść zależy od sposobu (miejsca, czasu) prowadzenia działalności gospodarczej. Jak słusznie zauważa Sybilla Stanisławska- Kloc treść i zakres postępowania zgodnego z dobrymi obyczajami należy oceniać osobno do każdego przypadku.<sup>304</sup>

Trudno znaleźć także przepis zakazujący przejmowania i wykorzystywania wyników (nietwórczych) cudzej pracy. Sybilla Stanisławska- Kloc uważa, iż można ewentualnie zastanawiać się nad wywiedzeniem podobnych zakazów z tzw. klauzul konkurencyjnych uregulowanych m.in. w kodeksie pracy (art. 100<sup>1</sup> - 101<sup>4</sup>)<sup>305</sup>.

W odniesieniu do przejmowania baz danych w Internecie z czynem nieuczciwej konkurencji będziemy mieli do czynienia gdy:

- systematyczne przejmowanie elementów lub całości baz danych przez firmę będzie następnie udostępnione przez konkurencyjny podmiot na rynku w krótkim odstępie czasu od wprowadzenia do obrotu pierwotnej bazy
- przejęcie jest jednokrotne lecz jest ono wierne a dokonane zmiany zawartości są minimalne i nie pociągają za sobą kosztów<sup>306</sup>.

---

<sup>301</sup> Por. S. Stanisławska- Kloc, *Ochrona baz danych w świetle przepisów prawa*, [w:] R. Skubisz, *Internet-problemy prawne*, op. cit., s.47 oraz teje: *Problematyka ochrony „tradycyjnych” i „elektronicznych” baz danych*, „Radca Prawny” 02/53, 03-04 2001.

<sup>302</sup> Por. J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.283.

<sup>303</sup> Ibidem.

<sup>304</sup> Zob. S. Stanisławska- Kloc, *Ochrona baz danych w świetle przepisów prawa*, [w:] R. Skubisz, *Internet-problemy prawne*, op. cit., s.48.

<sup>305</sup> Ibidem.

<sup>306</sup> Za S. Stanisławska- Kloc, *Ochrona baz danych w świetle przepisów prawa*, [w:] R. Skubisz, *Internet-problemy prawne*, op. cit., s.49. Zob. także więcej na temat *commercial immorality*.

Artykuł 3 ustawy z dnia 04.02.1994 r. o prawach autorskich i prawach pokrewnych stanowi, iż *bazy danych są przedmiotem prawa autorskiego nawet jeśli zawierają materiały nie chronione, o ile przyjęty w nich dobór, układ czy zestawienie ma twórczy charakter, bez uszczerbku dla praw do wykorzystywanych utworów.*

Tym samym poprzez przytoczenie treści przepisu art. 3 przeszedłem do uregulowania ochrony baz danych w polskim prawie autorskim Zbiór materiałów stanowi przedmiot prawa autorskiego jeśli wykazuje twórczy charakter, może się on przejawiać w doborze, układzie czy też w zestawieniu<sup>307</sup>. Podkreśla się, iż nie ma tutaj znaczenia nakład pracy, koszty oraz nazwa przyjęta dla takiego zbioru.

Polskie prawo autorskie rozróżnia wyraźnie „twórcze” i „nietwórcze” banki danych. Decydującą rolę odgrywa tu kryterium twórczości. Jako utwór baza danych uzyska ochronę tylko wtedy, gdy rezultat pracy, choćby nie otrzymał jeszcze ostatecznej postaci, wykazuje już ową cechę „własnej intelektualnej twórczości” autora<sup>308</sup>. Przejawia się ona (ta cecha) w sposobie wybierania czy porządkowania elementów składowych. Samo oryginalne kryterium doboru powstaje przeważnie przed rozpoczęciem zbierania materiałów. Problemem jest tu jednak to, iż w przypadku baz danych wyrażenie owej idei-pomysłu wymaga takiego rodzaju pracy, który ma charakter rutynowy choćby nawet były niezbędne ku temu wysokie kwalifikacja i duży nakład pracy.

Autorzy książki *Internet a prawo* wskazują ponadto, iż budowanie bazy danych według pewnych założeń dokonuje się dzięki pracy typowej, wolnej od indywidualnych wyborów. Stwarza to kolejną trudność w określeniu czasu. W którym powstaje dany utwór.<sup>309</sup> Na bazę danych mogą składać się następujące „utwory”:

1. objęte ochroną autorsko prawną,
2. utwory w stosunku, do których owa ochrona (praw majątkowych) wygasła,
3. wyjęte spod ochrony na mocy art. 4 ustawy,
4. m.in. opracowania dokumentacyjne, dane liczbowe, faktograficzne, materiały nie spełniające cech utworu w rozumieniu ustawy.

Kolejnym problemem jest wykorzystywane utworów objętych autorsko prawną ochroną w bazach danych. Mogą być one inkorporowane w całości bądź w części. Może zaistnieć sytuacja, w której pomimo, iż utwór jako taki jest chroniony, to ze względu na charakter przejmowanej z niego zawartości nie można mówić o naruszeniu prawa autorskiego.<sup>310</sup>

---

<sup>307</sup> Nie można doszukiwać się takiego charakteru :

- a) w doborze materiałów, informacji gdy dobór taki jest całkowicie wyczerpujący, zdeterminowany celem zbioru, czy też ma oczywisty charakter- np. książki telefoniczne, adresowe, katalogi towarów, firm, wykazy cen, indeksy osobowe i rzeczowe
- a) w zestawieniu informacji lub materiałów, gdy zestawienie ma oczywisty charakter i oparte jest na np. kryterium alfabetycznym, chronologicznym – J. Barta, R. Markiewicz, *Ochrona baz danych w systemie prawa autorskiego- stan obecny i perspektywy*, materiały konferencyjne „Infobazy '97 bazy danych dla nauki”, s. 23.

<sup>308</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.291.

<sup>309</sup> Ibidem, s. 292.,

Na gruncie procesu tworzenia bazy danych powstaje także sprawa podmiotu uprawnionego. Mogą znaleźć tu zastosowanie art. 9,12 czy też 14 prawa autorskiego.

<sup>310</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.292-193.

Osobne zagadnienie stanowi wykorzystywanie w bazach danych materiałów objętych dozwolonym użytkowaniem<sup>311</sup>. Czy można w oparciu o te przepisy stosować w bazach danych (a następnie udostępniać) utwory chronione prawem autorskim? Połowicznie tę kwestię wyjaśnia art. 29 ust 1 pr. aut.<sup>312</sup>

Nieostre kryterium „prawa gatunku twórczości” przyjęte w przepisie nie pozwala niejednokrotnie odrzucić stosowanie tego typu praktyki (np. budowanie baz danych z fragmentów utworów objętych ochroną praw autorskich, cytaty czy też inne fragmenty utworów). Janusz Barta i Ryszard Markiewicz zwracają także uwagę na inny aspekt dozwolonego użytku- swobodę korzystania przez osoby trzecie z takich baz oraz zamieszczonych w nich utworów. Do objętych prawem autorskim baz danych należy, *de lege lata*, odnosić także do postanowień, które dotyczą utworów ogólnie. Zauważają również, iż czynnikiem korygującym może być tylko klauzula art. 25 pr. aut. – dozwolony użytek nie może naruszać normalnego korzystania z utworu lub godzić w słuszne interesy twórcy.

## Ochrona baz danych w Unii Europejskiej

Duży wpływ na polskie prawo autorskie ma proces harmonizacji przepisów z uregulowaniami Unii Europejskiej, a mianowicie z przejęciem *sui generis* ochrony baz danych. Wzrost znaczenia baz danych nastąpił wraz z rozwojem i upowszechnieniem się Internetu. Są bowiem one immanentnie związane z sieciami komputerowymi. Niedostosowanie dotychczasowego prawa autorskiego (uświadomiono to sobie wyraźnie po orzeczeniu w sprawie Feist – piszę o nim w dalszej części pracy) skłoniło Unię Europejską do wypracowania jednolitego rozwiązania dla banków danych.

Dyrektywa UE z 11.03.1996 r.<sup>313</sup> już w preambule powołuje się na podstawową przyczynę tej regulacji a mianowicie na konieczność ujednoczenia prawa we wszystkich państwach członkowskich oraz na potrzebę wprowadzenia swobody w dostarczaniu towarów i usług „wyprodukowanych” na podstawie baz danych lub zawierających takie bazy<sup>314</sup>. Uwzględniono również to, aby wszystkie działania zmierzające do przyznania ochrony bazom danych nie przyczyniły się do powstania monopolu na fakty czy inne dane. Innym celem owego rozwiązania jest prowadzenie nowych uprawnień niezależnych od prawa autorskiego oraz nienaruszanie jakichkolwiek praw związanych z dobrami niematerialnymi inkorporowanymi do baz danych<sup>315</sup>.

Tekst dyrektywy owym zakazem obejmuje ochronę baz danych w każdej postaci- tak elektronicznej jak i innej. Nie jest więc istotna forma w jakiej wyprodukowano czy udostępniono bazę danych<sup>316</sup>. Pojęcie bazy danych obejmuje zbiór niezależnych utworów, danych lub innego rodzaju materiałów, uporządkowanych w sposób systematyczny lub metodyczny, dostępnych

<sup>311</sup> Patrz: przepisy rozdziału 3 oddział 3 ustawy o pr. aut.

<sup>312</sup> Zob. więcej na ten temat: J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.293.

<sup>313</sup> Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases *Official Journal L 077*, 27/03/1996 p. 0020 – 0028.

<sup>314</sup> S. Stanisławska- Kloc, *Ochrona baz danych w świetle przepisów prawa*, [w:] R. Skubisz, *Internet- problemy prawne*, op. cit., s.43.

<sup>315</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.296-297.

<sup>316</sup> Zob. J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.297.

indywidualnie przy pomocy środków elektronicznych lub innych ( art.1 dyrektywy UE). Wprowadzono również cztery kategorie banków danych:

- a) bazy podlegające ochronie prawa autorskiego oraz ochronie *sui generis*,
- b) bazy podlegające ochronie prawa autorskiego lecz taką ochroną nie objęte ze strony *sui generis*,
- c) nie podlegające ochronie prawa autorskiego lecz objęte ochroną *sui generis*,
- d) utwory nie kwalifikujące się do żadnej z tych dwóch kategorii ochrony prawnej.

Ochronie prawno autorskiej będą podlegały te bazy danych, które z powodu wyboru, uporządkowania ich zawartości stanowią własną intelektualną twórczość autora. Tylko więc twórcze wyrażenie bazy danych podlega ochronie prawa autorskiego

Ad c) W stosunku do takich banków danych (nietwórczych) objęto je ochroną, chociaż według prawa autorskiego nie są one utworami. Przedmiotem tej ochrony są one za względu na istotną inwestycję (ilościową i jakościową). Może ona przejawiać się w nakładach finansowych, może być związana z organizowaniem pracy zespołu badawczego.

Ważną kwestią jest zakres ochrony *sui generis* takich nietwórczych banków danych. Treścią tej ochrony są dwa uprawnienia, które możemy łącznie nazwać prawem zakazu (możność sprzeciwienia się) przejmowania i wykorzystywania danych. Systematyczne lub inaczej powtarzające się wykorzystywanie (*re-utilization*) drobnych części bazy jest określone jako nieistotna eksploatacja. Prawo to ma charakter bezwzględny i może stać się przedmiotem umów rozporządzających i licencyjnych. Jest przy tym niezależne od ochrony zawartości bazy, która wynika z prawa autorskiego czy innego prawa wyłącznego<sup>317</sup>. Jak podkreślają autorzy pracy *Internet a prawo* istotnym novum w dyrektywie jest to, iż w razie pobrania i powtórnego wykorzystania całej lub części zawartości cudzej bazy działanie takie będzie stanowiło naruszenie prawa nawet wówczas, gdy przejęto elementy nietwórcze (dotyczy to banków danych będącymi utworami w rozumieniu prawa autorskiego oraz tych korzystających tylko z ochrony *sui generis*).

Widzimy więc, że przepisy dyrektywy pozwalają legalnemu użytkownikowi (takim pojęciem posługuje się dyrektywa) w dowolnym celu pobranie i powtórne wykorzystanie jedynie nieistotnych części bazy- dotyczy to jednak tylko takich baz danych, które udostępniono publicznie<sup>318</sup>. Przewidziany został 15- letni okres ochrony *sui generis* (art. 10). Liczy się go od początku roku następującego po roku, w którym bank danych ukończono.

---

<sup>317</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.304.

<sup>318</sup> Pojawiają się tu dwa zakazy:

1. nie mogą być dokonywane czynności pozostające w sprzeczności z normalną eksploatacją albo które prowadzą do nieusprawiedliwionego naruszenia słuszych interesów producenta,
1. wyłączone jest takie postępowanie, prowadzące do naruszenia prawa autorskiego lub praw pokrewnych do materiałów zgromadzonych w bazie.

Podział za: Barta, R. Markiewicz, *Internet a prawo*, op. cit., s.305.

Bazy danych i ich ochrona stanowiły i chyba nadal są jednym z zasadniczych zagadnień w całym prawie autorskim. Przejawia się to w całym szeregu orzeczeń, które dotyczą właśnie tej materii.

Najważniejszym z nich jest orzeczenie w sprawie Feist<sup>319</sup>. Sporna stała się książka telefoniczna a właściwie jej część określana mianem *white pages* (umieszczane są w niej w układzie alfabetycznym dane dotyczące abonentów – nazwiska, adresy i oczywiście numery telefonów). Sąd oddaliwszy powództwo o naruszenie prawa autorskiego stwierdził, że nie ma podstawy do uznania, iż przejęcie zawartości wspomnianej części książki naruszyło prawa autorski powoda. Przedmiotem sporu nie jest utwór (w rozumieniu prawa autorskiego) za względu ma brak cechy twórczości. Orzeczenie sądu pierwszej instancji było zgoła inne. W orzeczeniu Sąd Najwyższy USA określił, iż warunkiem *sine qua non* ochrony autorsko prawnej jest oryginalność<sup>320</sup>. Fakty nie podlegają ochronie i mogą być dowolnie wykorzystywane. Sąd jednocześnie nie pozbawił ochrony autorsko prawnej takich baz, które zawierają tylko proste dane (fakty) dopóki wybór i układ jest wystarczająco twórczy. Orzeczenie w sprawie Feist zrywa z doktryną „spoczonego czoła”, która do tej pory (czyli do roku 1991 r.) dominowała w Stanach Zjednoczonych. Przyznaje także, iż zawartość baz danych może być przejmowana i wykorzystywana ponownie dopóki wraz z zawartością nie zostanie przejęty twórczy układ czy uporządkowanie danych. Orzeczenie to było istotne ze względu na jego precedensowy charakter. Jego doniosłość podkreślono nawet w preambule dyrektywy UE o prawnej ochronie baz danych.

Problematyka ochrony baz danych oraz adresów internetowych jak widzimy jest głośno dyskutowana na łonie opracowań naukowych prawa autorskiego. Na naszych oczach powstają nowe uregulowania, które będą stanowiły model i podstawę dla przyszłych przepisów. Stosunkowo nowe dziedziny, które wykształciły się w Internecie, które dzięki niemu otrzymały nieznane oblicze pozostają w centrum zainteresowania prawa autorskiego.

Prawo w znaczący sposób ingeruje w Internet lecz samo nie pozostaje wolne od jego wpływów. Zauważyć to można przede wszystkim śledząc aktualne wydarzenia na polu prawa autorskiego.

---

<sup>319</sup> Feist Publications Inc. Vs. Rural telephone Service Co. Inc. US- Supreme Court 89/909,27.03.1991 r. Zamieszczone w GRUR Int,1991/8,s.933 i nast.

<sup>320</sup> S. Stanisławska- Kloc, *Ochrona baz danych w świetle przepisów prawa*, [w:] R. Skubisz, *Internet- problemy prawne*, op. cit., s.36.

## Zakończenie

Spostrzeżenia, które przedstawiłem w niniejszej pracy wskazują jednoznacznie, iż wpływ Internetu na prawo jest znaczny. Przystosowania systemów prawnych do zdobyczy technik informatycznych i telekomunikacyjnych należy dokonywać z uwzględnieniem osiągniętego dorobku kultury prawniczej, jak ochrona prywatności, dóbr osobistych czy autorskich, oraz zapewnić, aby owe rozwiązania nie były tymczasowe. Należy więc tworzyć prawo elastyczne. Gotowe do przystosowania się, do wchłonięcia nowych osiągnięć ery informatycznej.

Zmiany dokonujące się na naszych oczach można nazwać w pewien sposób rewolucją informatyczną. Rewolucją, która oddziałuje na wiele dziedzin naszego życia. Prawo nie pozostaje wolne od wpływu Internetu i sieci komputerowych. Trudno nie dostrzec, iż nowe techniki informatyczne i komunikacyjne mają wpływ na podstawowe prawa człowieka, w pierwszym rzędzie na wolność wypowiedzi i prawo do informacji<sup>321</sup>. Jak więc w owych warunkach te prawa i wolności mają być zapewnione i realizowane? Pamiętać trzeba o potrzebie utrzymania pluralizmu informacyjnego, uwzględniania wielości kultur, o ochronie praw dzieci i młodocianych przed szkodliwymi treściami. Internet oddziałuje, jak mogliśmy się przekonać, na wiele gałęzi prawa. Uwzględnienie przede wszystkim prawa międzynarodowego oraz prawa Unii Europejskiej w tej materii wskazuje na konieczność wspólnych międzypaństwowych rozwiązań. Autorzy książki *Internet a prawo* mówią wręcz o potrzebie wykreowania prawa cyberprzestrzeni. W zderzeniu prawa z Internetem widzimy, iż wymyka się on spod jakichkolwiek klasyfikacji, przekracza granice państwowe. Nie można zatem bazować na wypracowaniu rozwiązań dla jednego państwa.

Dialog polityczny i prawniczy, który odbywa się na różnorodnych forach zmierza w kierunku zapewnienia podstaw do rozwoju jednakowych dla wszystkich podmiotów. Ma również na celu eliminację zagrożeń, które bezpośrednio i pośrednio kreuje Internet.

Legislatorzy powinni jednak działać w miarę ostrożnie dokonując analizy z odpowiednim wyprzedzeniem skutków zmian. Już dziś możemy dostrzec ich symptomy, zdają się one niebezpieczne w zakresie prawa, które w społeczeństwie informacyjnym powinno być w szczególności w sposób preferowane. W pracy starałem się przedstawić nie tylko wypracowane rozwiązania lecz także projekty, które już w przyszłości będą obowiązującym prawem, trudność polegała na tym, iż w stosunku do związków Internetu z prawem nie ma jednolitych standardów. Prawo w tej kwestii nie dysponuje bogatym orzecnictwem, jest to proces nowy, który musi opierać się na nowoczesnych rozwiązaniach. Starałem się również wykazać, iż ogromne korzyści niesione przez sieć mogą być przysłonione również wielkimi zagrożeniami. Przedstawiłem je między innymi w prawie konstytucyjnym (problem kontroli informacji, ograniczenia wolności słowa), w prawie karnym (nowe przestępstwa czy też nowe formy już znanych przestępstw), w prawie autorskim (kwestia ochrony praw autorskich) czy też w materii tak specyficznej dla Internetu jaką są bazy danych i adresy internetowe.

---

<sup>321</sup> J. Barta, R. Markiewicz, *Internet a prawo*, op. cit., s. 320.

Stopień prac nad rozwiązaniami mającymi choć w części poddać Internet przepisom prawnym jest różny w wielu dziedzinach. Często dopiero podstawy pod przyszłe ustawodawstwo się tworzą – czy tworzyły w trakcie pisania tej pracy jak na przykład w przedmiocie podpisu elektronicznego w prawie polskim. Konieczność uwzględnienia nie tylko aktualnego stanu prawnego lecz również prac legislacyjnych była nie lada wyzwaniem.

Większym z kolei jest przewidzenie kierunku owych zmian. W jaką stronę będzie zdążało ustawodawstwo regulujące materię Internetu (na przykład w prawie autorskim- kwestia dozwolonego użytku)? Trudno dziś odpowiedzieć na to pytanie. Z jednej strony należy pamiętać o wszystkich osiągnięciach w tej dziedzinie, z drugiej zaś konieczne staje się uwzględnienie czynnika, który ma na prawo duży wpływ, jak starałem się wykazać.

Czynnikami tym są nowoczesne technologie informatyczne i telekomunikacyjne. Postęp techniczny jest tak znaczny, iż przyszłość będzie należała do rozwiązań prawnych elastycznych i otwartych na zmiany. Samo prawo kształtuje się powoli. Nowe instytucje nie pojawiają się nagle. Rozwiązania poparte są latami doświadczeń i obserwacji. Problem z Internetem polega na tym, że jest to wynalazek najszybciej się rozprzestrzeniający i mający tak ogromny wpływ na prawo. Aby nadążyć za wszelkimi zmianami prawo będzie musiało szybciej dostosowywać swe instytucje do rzeczywistości<sup>322</sup>. Rzeczywistości, która już dziś staje się nierzeczywista (wirtualna).

---

<sup>322</sup> Może nawet w systemie ustawodawczym konieczne będą zmiany z uwagi na dzisiejszą czasochłonność tego procesu wiążącą się z dużymi kosztami oraz małym stopniem przystosowywania się prawa do otaczających realiów.

## Wykaz aktów prawnych.

### Polskie akty prawne.

1. Konstytucja Rzeczypospolitej Polskiej z 02.04.1997.
2. Kodeks cywilny z 1964.04.03 Dz.U.64.16.93.
3. Kodeks postępowania cywilnego z 1964.11.17 Dz.U.64.43.296.
4. Prawo międzynarodowe prywatne z 1965.11.12 Dz.U.65.46.290.
5. Kodeks pracy z 1974.06.26 Dz.U.98.21.94.
6. Ustawa o księgach wieczystych i hipotece z 1982.07.06 Dz.U.82.19.147.
7. Prawo prasowe z 1984.01.26 Dz.U.84.5.24.
8. Ustawa o zwalczaniu nieuczciwej konkurencji z 1993.04.16 Dz.U.93.47.211.
9. Ustawa o prawie autorskim i prawach pokrewnych z 1994.02.04. Dz.U.00.80.904 j.t.
10. Ustawa o rachunkowości z 1994.09.29 Dz.U.94.121.591.
11. Kodeks karny z 1997.06.06 Dz.U.97.88.553.
12. Kodeks postępowania karnego Dz.U.97.88.555.
13. Ordynacja podatkowa z 1997.08.29 Dz.U.97.137.926.
14. Prawo bankowe z 1997.08.29 Dz.U.97.140.939.
15. Kodeks karny skarbowy z 1999.09.10 Dz.U.99.83.930.
16. Ustawa o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny z 2000.03.02 Dz. U. nr 22 poz. 271.

### Zagraniczne akty prawne.

- Europejskie akty prawne i inne dokumenty

1. Dyrektywa 85/577 EWG z 20.12.1985 r. w sprawie ochrony konsumentów przy umowach zawieranych poza miejscem prowadzenia handlu.
2. Dyrektywa Parlamentu i Rady Wspólnot Europejskich 97/7 z 20.05.1997 r. o ochronie konsumenta w umowach zawieranych na odległość (OJL 144/19 z 04.06.1997 r.
3. Directiv 1999/93/EC of the European Parliament and of the Council on 13. December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities z 19.01.2000 r.
4. Dyrektywa 2000/28/EC i 2000/46/EC w sprawie e-pieniędzy.
5. Directiv 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (Directiv on electronic commerce) Official Journal L 178.17/07/2000 p.0001-0016.
6. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases Official Journal L 077, 27/03/1996 p. 0020-0028.
6. Europa i społeczeństwo globalnej informacji, Zalecenia dla Rady Unii (Recommendations to the European Council „Europe and the global

- information society” z 16.05.1994 r. zauważyć należy, iż członkiem grupy (High- Level Group on the Information Society).
7. Plan działania Unii „droga Europy do społeczeństwa informacyjnego” - dokument Komisji z 19.07.1994 r. - COM (94)347 final.
  8. Commercial Communications in the Internal Market- Green Paper from the Commission COM (96)192, April 1996.
  9. Rekomendacja 97/489/EC dotycząca transakcji pokrywanych przez elektroniczne systemy płatności.
  10. Green Paper on Commerce COM (96)530, November 1996.
  11. Action Plan on promoting safer use of the Internet (decyzja nr 276/1999 EC, Europejskiego Parlamentu i Rady z 25.01.1999 r.
  12. eEurope An Information Society For All Communication on a Commission Initiative for the Special European Council of Lisbon 23-24 March 2000.

-Akty prawne i dokumenty innych państw i organizacji

1. Karta Narodów Zjednoczonych.
2. Konwencja Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów sporządzona w Wiedniu dnia 11.04.1980 roku.
3. Konwencja WIPO w sprawie ochrony artystów wykonawców i producentów fonogramów (WIPO Performances and Phonogram Treaty).
4. Konwencja WIPO dotycząca praw autorskich (WIPO Copyright Treaty).
5. Konwencja w sprawie handlowych aspektów praw własności intelektualnej (TRIPS).
6. Modelowa ustawa UNCITRAL, dotycząca zagadnień prawnych związanych z Elektronicznym Przekazem Danych (EDI) i pokrewnych środków komunikacyjnych. Zgromadzenie Ogólne Narodów Zjednoczonych w czerwcu 1996 roku na 29 sesji.
7. Rezolucja Zgromadzenia Ogólnego z listopada 1998 r. (53/22).
8. Konstytucja Stanów Zjednoczonych.
9. Federal Dillution Act z 1995 r. (15 U.S.C. 1125 (c)) (USA).
10. Ustawa federalna z 24.01.2000 r.- Electronic Signatures in Global and National Commerce Act (USA).
11. A Framework for Global Electronic Commerce z 01.07.1997 .
12. OECD Progresses Towards Achieving on International Consensus on the TAX Treatment of E-Commerce, Paryż 12.02.2001.
13. Towards A Global Information Society G 8 Global Information Society Pilot Projects Final Report.

**Orzecznictwo:**

1. Orzeczenie Sądu Najwyższego Stanów Zjednoczonych Ameryki z 26.06.1997 w sprawie Reno v. ACLU.
2. Sprawa Miller v. California, (413.US.15(1973)).
3. Sprawa Stanley v. Gorgia; por. Y. Akdeniz.

4. Postanowienie sądu apelacyjnego z 20.01.1999r.III Akz 13/99, KZS 1999/2/27 w Krakowie.
5. Intermatic Inc vs. Toeppen 96 C 1982, 1996 U.S. Dist. Lexis 14878 (ND III Oct. 3. 1996).
6. Panavision Intl L.p. vs. Toeppen 1996 WL 653736 (C.D. Calif. Nov. 05, 1996)
7. Wyrok Sądu Apelacyjnego w Warszawie z dn. 19.12.1995 r. sygn. I Acr 1013/95 OSA 1997/4.
8. Feist Publications Inc. Vs. Rural telephone Service Co. Inc. US- Supreme Court 89/909,27.03.1991 r. Zamieszczone w GRUR Int,1991/8, s.933 i nast.

## **Bibliografia.**

### **Wydawnictwa zwarte:**

1. Adamski A, Prawo karne komputerowe, Warszawa 2000.
2. Adamski A., Przepisy prawa komputerowe w nowym kodeksie karnym,[w:]Nowa kodyfikacja karna. Kodeks Karny, krótkie komentarze. Zeszyt 17, Warszawa 1998.
2. Barta J., Markiewicz R., Internet a prawo, Kraków 1998.
3. Barta J., Markiewicz R., Prawo autorskie, Warszawa 1998.
4. Barta J., Markiewicz R., Komentarz do ustawy o prawie autorskim (...), Warszawa 1995.
5. Chmiela W., Systemy elektronicznej bankowości i cyfrowej płatności, Warszawa 1999.
6. Chobot A., Nowe formy zatrudnienia, Warszawa 1997.
7. Gardocki L., Prawo karne, Warszawa 1998.
8. Grajewski J., Peprzycki L.K, Kodeks Postępowania Karnego z komentarzem, Sopot 2000.
9. Grzegorzczak T., Tylman J., Polskie postępowanie karne, Warszawa 1999.
10. Kocot W., Zawieranie umów sprzedaży według Konwencji Wiedeńskiej, Warszawa 1998.
11. Majchrzycka-Guzowska A., Finanse i prawo finansowe, Warszawa 1998.
12. Nowacki J., Prawo publiczne - prawo prywatne, Katowice 1992.
13. Nowa kodyfikacja karna. Krótkie komentarze, Warszawa 1997.
14. Kodeks postępowania cywilnego - komentarz tom I , pod red. K. Piaseckiego, Warszawa 1999.
15. Kodeks Cywilny Komentarz Tom I pod red. K. Pietrzykowskiego, Warszawa 1999.
16. Pyziół W., Prawo bankowe- komentarz- praca zbiorowa, Warszawa 1999.
17. Radwański Z., Prawo cywilne- część ogólna, Warszawa 1999.
18. Redelbach A., Wstęp do prawoznawstwa, Poznań 1996.
19. Skubisz R. (red.): Internet- problemy prawne, Lublin 1999.
20. System prawa cywilnego tom I, część ogólna, Wrocław, Warszawa, Gdańsk, Łódź 1985.
21. Wronkowska S., Ziemiński Z., Zarys teorii prawa, Poznań 1997.
22. Zieliński A., Postępowanie cywilne, Warszawa 2000.

## Czasopisma:

1. Adamczyk M., Elektroniczny podatek, tygodnik „Wprost” z 16.04.2000.
2. Adamski A., P.S./1998/11-12/149.
3. A.my, PIT wysłany mailem, „Rzeczpospolita” z dn. 20.04.2001.
4. Ćwiklak D., Bienias T., konsultacja Donajski J. Encyklopedia Internet 1/ Narodziny sieci, MAGAZYN nr 5 dodatek do Gazety Wyborczej nr 28, 2000/02/03.
5. Domaszewicz Z., Plamy w sieci, „Gazeta Wyborcza” z dn. 15.09.2000.
6. Fedorowicz H., Wycofać się łatwo, lecz trzeba wiedzieć kiedy, „Rzeczpospolita” z dn. 04.01.2001.
7. Gajos, Niech rozsądzi nas arbiter, „Rzeczpospolita” z dn. 30.11.2000.
8. Giziński J., Strażnicy sieci, „Wprost” z dn. 21.05.2000.
9. Hoeren Th., The Green Paper on Copyright and Related Rights in the Information Society, EPIR 1995/10, s.514.
10. Jermiołowski A., Sieciowy terroryzm, „Rzeczpospolita” z dn. 10.02.2000.
11. Kamiński R., Internet poza prawem, „Wprost” z 20.01.2000.
12. Karolek J., Elektroniczni obywatele, „Wprost” z 22.02.2000.
13. Knoppek K., Wydruk komputerowy jako dowód w procesie cywilnym, „Państwo i Prawo” 1993/2/54.
14. Kort K., Dzikie osadnictwo w sieci, „Gazeta Wyborcza” z 06.03.2000, przedruk z „Wall Street Journal Europe”.
15. Kościelniak P., Zamiast kaset i kompaktów, „Rzeczpospolita” z 16.03.2000.
16. Kościelniak P., Porno problem, „Rzeczpospolita”, 16.03.2000.
17. Kościelniak P., Filmy na życzenie, „Rzeczpospolita” z dn. 28.12.2000.
18. Kuresz K., Papiery wartościowe przez Internet, „Rzeczpospolita” z 26.07.2000.
19. Kurzępa B., Kontrola i utrwalanie rozmów telefonicznych wg k.p.k., Prok. I PR. 1999/3/77.
20. Lewandowska J., Ciekawość przyczyną zwolnienia, „Rzeczpospolita” z dn. 26.02.2001.
21. Makarenko V. TV Internet- oferta polskich stacji telewizyjnych,, „Gazeta Wyborcza” z 27.12.2000.
22. Makarenko V., TV Internet, „Gazeta Wyborcza” z 27.12.2000.
23. Makarenko V. Najpierw Kraków i Warszawa, wywiad z E.Kurek. „Gazeta Wyborcza” z 27.12.2000.
24. Maniecki M., Szanse i zagrożenia, „Teleinfo” z 25.09.2000 r., nr 39/2000, s.33.
25. Marciński, W. E-rady dla Europy, „Teleinfo” z 25.09.2000 r., nr 39/2000, s.33-34.
26. Matlak A., Prawo autorskie i prawa pokrewne w społeczeństwie informacyjnym z punktu widzenia projektu nowej dyrektywy Unii Europejskiej, „Radca Prawny” 01/2001.
27. Mikołajewska B., Sieć na sieć, „Polityka” z dn. 28.10.2000.
28. Myczkowska, A. Bank www, „Rzeczpospolita” z 26.07.2000.
29. Myczkowska A., Rachunek w sieci, „Rzeczpospolita” z 15.11.2000.
30. Myczkowska A., Banki przejmują odpowiedzialność, „Rzeczpospolita” z 09.02.2001.
31. Myczkowska A., Dobrze tylko dla banków, „Rzeczpospolita” z 17-18.02.2001.

32. Niklewicz K., Najpierw prawo, potem boom, „Gazeta Wyborcza” z 10.04.2000.
33. Ożogalska J., Prawne problemy posługiwania się adresami (domenami) internetowymi w obrocie gospodarczym, „Radca Prawny” 01/2001.
34. Palarczyk J., Jak podzielić złote jajo, „Gazeta Wyborcza” z 09.03.2000.
35. Pawlicki J., Jak dogonić Amerykę, „Gazeta Wyborcza” z 24.03.2000.
36. R. Perera, A step closer to becoming law, „Infoworld” z 25.04.2001.
37. Raszowska G., Nie w biurze i nie na etacie, „Rzeczpospolita” z dn. 13.12.2000.
38. Rybarczyk M., Tu Wielki Brat, „Gazeta Wyborcza” z 04.12.2000.
39. Seib G.E., Vandehei J., Amerykańskie pospolite ruszenie na rzecz opodatkowania sieci, „Wall Street Journal”, przetłum. przez J. Skup, „Gazeta Wyborcza” z 03.07.2000.
40. Sitnicki I., Srebrny M., Jak podpisuje się świat, „Rzeczpospolita” z 09.02.2001.
41. Sitnicki I., Srebrny M., Nie taki diabeł straszny jak go malują, „Rzeczpospolita” z 08.02.2001.
42. Sowela G., Zmi.ana adre.su, „Rzeczpospolita” z dnia 23.11.2000.
43. Stosio A., Kto kliknie więcej, „Rzeczpospolita” z 03.01.2000.
44. Świderek T. , Mniej odwiedzających mniej pieniędzy, „Rzeczpospolita” z dn.11.02.2000.
45. Świerczyński M., Jak napój z automatu, „Rzeczpospolita” z 30.11.2000.
46. Urbański K.B., Chroń swój komputer, „Rzeczpospolita” z dn.15.05.2000.
47. Wojciechowski J., Despotom nie, „Rzeczpospolita” z dnia 28.11.2001.
48. Zakrzewski R.: art. M.Prawn. 1998/10/378.
49. R. Zasuń, *Fiskus królowej Beatrycze*, „Gazeta Wyborcza” z 11.12.2000.
50. Ziętkiewicz, Chroń go sam, „Rzeczpospolita” z dn. 20.02.2001.
51. ZUM, Niebanalne bannery, „Gazeta Wyborcza” z dn. 30.10.2000.
52. Zwierzchowski Zb., Rozkradana informatyka, „Rzeczpospolita” z 26.05.2000.

## Inne.

1. J. Barta, R. Markiewicz, Ochrona baz danych w systemie prawa autorskiego- stan obecny i perspektywy, materiały konferencyjne „Infobazy '97 bazy danych dla nauki”, s. 23.
2. A Brief History of the Internet, na stronie WWW:  
<http://www.isoc.org/internet/history/brief.html>.
3. Computer- Related Crime: Recommendation No.R(89)9 on the computer related crime and final report of the European Committee on Crime Problems. Council of Europa, Strasbourg 1990.
4. Copper J., E-commerce: impact and policy challenges ECO/WKP(2000)25
5. Creed A., Australian state may bring courts procedures online, „Newsbytes”, 04.01.2001.  
<http://www.newsbytes.com/news/01/160072.html>.
6. Dryden J., The work of the OECD on Electronic Commerce.
7. Global Information Infrastructure- Global Information Society- GII-GIS Policy Recommendations for action OECD 1997.

8. Kliś M., Martiuszek T., Przepisy prawa elektroniczne, tekst dostępny na serwerze [www.vagla.eu.org](http://www.vagla.eu.org).
9. Kliś M., Przepisy prawa w Internecie. Zagadnienia podstawowe, s.12, dokument dostępny w Internecie na serwerze [www.vagla.eu.org](http://www.vagla.eu.org).
10. Konarski X., Prawo cywilne a Internet, „Biznesnet” z 17.10.2000 r. , artykuł dostępny na stronie: <http://www.biznesnet.pl/index.phtml?pg=ebiz&a=455>
11. Loundy D.J., A Primer on Trademarks Law and Internet Addresses, 15 John Marshal J. OfComputer and Info Law 465(1997).
12. OECD Progresses Towards Achieving an International Consensus on the TAX Treatment of E-Commerce, Paryż 12.02.2001 r. [www.oecd.org/media/relase/nw01-15a.htm](http://www.oecd.org/media/relase/nw01-15a.htm).
13. Satko J., glosa OSP 199/3/66 do postanowienia SN z dn. 20.10.1998, III Kz 182/98.
14. Towards A Global Information Society G 8 Global Information Society Pilot Projects Final Report.  
Dokument dostępny na stronie [www.gip.int/g8/mainreport.htm](http://www.gip.int/g8/mainreport.htm).

#### Strony WWW:

1. [www.digicash.com](http://www.digicash.com)
2. [www.ecommerce.gov](http://www.ecommerce.gov)
3. <http://www.iss.net>.
4. <http://www.mf.gov.pl>
5. <http://www.netsizer.com>
6. <http://www.nbp.pl/>
7. <http://www.pit.pl/>
8. <http://www.ustreas.gov/>
9. <http://www.vagla.pl/>
10. [www.vagla.eu.org/projekt\\_mswia.htm](http://www.vagla.eu.org/projekt_mswia.htm).
11. <http://www.vat.pl/>
12. <http://www.zus.gov.pl/>

#### Wykaz tabel:

1. Tabela 1: Społeczeństwo informacyjne w 1999/2000 r. (w milionach).
2. Tabela 2. Statystyka domen w ostatnich 4 tygodniach z rozbiciem na główne domeny funkcyjne.

